

E Safety Policy

(SP)

Document Control

Document Title: E Safety Policy

Document Number: P28

Author: Quality Assurance Team

Change Authority: The Board of Directors

Change History

Version	Date	Reason for change	Change by
0.1	01 st January 2015	First draft	
1.0	11 th January 2016	Company Review	Quality Assurance Team
1.1	18 th February 2016	Company Review	TM/LD/FR
1.2	20 th January	Company Review	Quality Assurance Team
1.3	22 nd April 2019	Company Review	Quality Assurance Team

E-Safety Policy

Writing and reviewing the E-safety policy

This E-safety Policy is part of Global London College Development Plan and relates to other policies including those for ICT, bullying and for child protection.

E-safety (The Principal)

➤ Our E-safety Policy has been written by the college, building on best practice and government guidance. It has been agreed by senior management and approved by Directors.

➤ The E-safety Policy and its implementation will be reviewed annually

➤ The E-safety Policy has been discussed by Staff.

➤ The E-safety Policy will be discussed by the College Council

➤ The college has identified a member of staff who has an overview of the E Safety policy

➤ The E-safety Policy was revised by: the teaching staff and Directors.

➤ It was approved by the Board of Directors

Teaching and learning

Why Internet and digital communications are important

➤ The Internet is an essential element in 21st century life for education, business and social interaction. The college has a duty to provide students with quality Internet access as part of their learning experience.

➤ Internet use is a part of the curriculum and a necessary tool for staff and students.

➤ Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

➤ Students will be educated in the effective use of the Internet

➤ Students will be shown how to publish and present information appropriately to a wider audience.

Students will be taught how to evaluate Internet content

➤ The college will seek to ensure that the use of Internet derived materials by staff and by students complies with copyright law.

➤ Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. (Awareness of college plagiarism policy)

➤ Students will be advised how to report unpleasant Internet content.

Managing Internet Access

Information system security

- College ICT systems security will be reviewed regularly (College in process upgrading internet access and data storage on Cloud)
- Virus protection will be updated regularly (Annual update AVG antivirus)
- Students and staff may only access relevant academic data produce by GLC
- Students must immediately tell a teacher if they receive offensive e-mail and a hard copy will be requested.
 - Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to student email communication must only take place via a college email address or from within the learning platform and will be monitored.
 - Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The college will consider how e-mail from students to external bodies is presented and controlled.

Published content and the college web site

- The contact details on the Web site should be the college address, e-mail and telephone number. Staff or students personal information will not be published.

Publishing photographs, images and work

- Photographs that include students will be selected carefully and may enable individual Students to be clearly identified.
- Student' full names will be avoided on the Web site (Without permission) or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Care for Under 18s: Written permission from parents or Accompanying Tutors will be obtained before photographs or images of students are published
 - Written permission from adults will be obtained before their names, photographs or images of themselves are published.

➤ Parents should be clearly informed of the college policy on image taking and publishing, both on college and independent electronic repositories. (See parents consent form)

Social networking and personal publishing on the college learning platform

- The college will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
- Students must not place personal photos on any social network space provided in the college learning platform without permission.
- Student, parents and staff will be advised on the safe use of social network spaces
- Student will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The college will work tirelessly to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, the site must be reported to the nominated member of staff (Director of Administration)
- The college will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised in regard for the students' age. Managing emerging technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in college is allowed.

Other devices

- Mobile phones and associated cameras will not be used during lessons or formal college time except as part of an educational activity and by staff only if a permission form has been completed and authorised by the Principal.

- The sending of abusive, offensive or inappropriate material is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the college use.
- Staff should not share personal telephone numbers with students and parents.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' (See staff files)
- The college will maintain a current record of all staff and pupils who are granted access to college ICT systems.
- Parents will be asked to sign and return a consent form (Currently not applicable).
- Students must agree to sign and comply with the Acceptable Use Policy before being granted Internet access.
- Any person not directly employed by the college will be asked to sign an 'acceptable use of college ICT resources' form before being allowed to access the Internet on the college site.

Assessing risks

- The college will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a college computer. The college cannot accept liability for material accessed, or any consequences of Internet access.
- The college will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff (See Student code of Conduct and Disciplinary Procedures).
- Any complaint about staff misuse must be referred to the head teacher. (See Staff Code of Conduct)
- Complaints of a child protection nature must be referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with college child protection procedures. (GLC Welfare officer and welfare support and Director of Administration)

- Students and parents will be informed of consequences for Students misusing the Internet.
- All use of the college Internet connection by community and other organisations shall be in accordance with the college E-safety policy.

Communications Policy

Introducing the E-safety policy to students

- Appropriate elements of the E-safety policy will be shared with students
- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

- All staff will be given the College E-safety Policy and its importance explained during staff Induction (See Staff files)
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support (Currently not Applicable)

- Parents and tutors/ carers attention will be drawn to the College E-safety Policy in newsletters, the college brochure and on the college web site.
- Parents and tutors / carers will from time to time be provided with additional information on:

E-safety.

- The college will ask all new parents, tutors/carers of under 18 year old students to sign the parent /student agreement when they register their child with the college.