COBIS MEMBER

CAMBRIDGE International Education

Cambridge International School

ENGLISH INTERNATIONAL SCHOOL OF TUNIS

British Curriculum

EIST Safer Internet and Social Media Policy 2025-2026

Revised Date:	April 2026
Next Review Due:	August 2026
Policy Reference Number:	EIST 2026 SISMP Ver.2

1. Rationale

The Cambridge International Computing curriculum, within the context of digital literacy, responsibility and safety, provides the necessary guidelines for teaching safer internet practice.

Its rationale emphasises the nurture and development of confident, responsible digital citizens who master age-appropriate computer science and digital literacy knowledge and skills. They are better equipped for life in a future of increasingly accelerative technological change.

It is for this reason that computing education and digital learning are central components of our school's academic offering.

Safety and responsibility are central to computing education: learners develop awareness of online risks, ethical use, and safe digital communication, promoting resilience, critical thinking, and global citizenship to navigate technology securely and inclusively.

This policy discusses procedures and systems designed to support these aims.

2. Aims and Objectives

This policy aims to provide direction and guidance in the monitoring of safer internet procedures, including the use of computing devices and IT infrastructure for teaching and learning across the curriculum, as well as support in computing education, safer internet and digital literacy at school.

Mastery of computer science and digital literacy requires more than just learning a repertoire of skills. Children must be encouraged to become discerning manipulators of computing technologies in all curriculum domains, including arts, humanities, languages, and sciences. They should experience a range of different applications, devices, environments, and games, to understand how they can be used, what they can be used for, their limitations and their power.

This policy provides guidance on achieving these aims responsively and safely.

3. Glossary and Terms

Computing, as a discrete curriculum domain, is a body of knowledge and understanding comprising a variety of processes and systems that handle electronically retrievable information. Computers and computing devices are the most obvious of these processes and systems, but the domain also includes (as far as is relevant to our pupils' education) the infrastructures and technologies of the internet and world wide web, all digital data, including private and public data used in machine learning and artificial intelligence (AI) education, all mobile technology communications, information retrieval and storage hardware and software, programmable robots and toys such as Lego Mindstorms, video games, creativity tools such as electronic musical instruments, science tools such as digital microscopes and telescopes, and photographic and reprographic devices (cameras, digital sound recorders, fabricators, optical scanners, printers, replicators, and video cameras).

4. Policy Statements

Syllabus

The overriding principle in computing education is the advantage, value, power, and mastery that computing technology provides to support diverse learning in digital and or virtual contexts. Pupils benefit from a wide range of learning opportunities in discrete computing lessons. Thus:

- All pupils from EYFS to Year 2 practise basic operations in file and printer management, and efficient use of inputs (keyboard and mouse so they can be ready and responsible;

- Pupils from Year 1 to Year 6 participate in mandatory digital literacy (and digital citizenship and safer internet) sessions throughout the year;
- Pupils from Year 7 to Year 12 participate in mandatory digital literacy (and digital citizenship and safer internet) sessions throughout the year, with the added rigour of the Cambridge syllabus.

Children will be taught how to use digital learning resources with confidence and autonomy, enabling their effective and productive integration with classroom, home, and virtual learning.

At school, and in addition to the statutory Cambridge programme of study for computing, pupils are taught:

- How to access the school's digital learning environment(s), and other virtual learning environments;
- How to chat;
- How to comment;
- How to edit online documents (including PDFs and slides);
- How to print;
- How to submit assignments;
- How to photograph an item;
- How to upload a photograph;
- How to manage a portfolio.

Services

Computer Labs

The school offers two computer labs which are fully equipped to deliver the programme of study for computing education. The computer lab's portfolio consists of:

- 29 personal computers;
- 10 tablet computers;
- School internet service

Bring Your Own Device

The school's Bring Your Own Device (BYOD) policy is designed to allow the use of personal devices in school in a way that enhances and supports teaching and learning. It also aims to protect children from harm, minimise risk to the school networks and explain what constitutes acceptable use or misuse of the BYOD policy.

Internet service

The school's internet service provider will ensure that, in accordance with the terms of the service level agreement, internet access conditions will always conform to expected quality.

The school will guarantee that security services (including filtering and firewall) and the ISP itself are continuously operational, and that outage reports are readily available.

The ISP's service level should conform to standards recommended by the UK Safer Internet Centre, and must conform to the prevailing (dominant) standards set by the DFE, in the September 2016 version of the document, *Keeping children safe in education: for schools and colleges*.

IT support personnel, whether employed by the school or otherwise, will comply with this policy and ensure that all infrastructure meets prevailing safety standards advised in this section of the policy.

The school will conform to statutory guidance published by the DFE, including the standards dictated by the October 2020 version of the document, *Remote education good practice*.

Internet communication

Pupils are provided by the school an access to a range of Microsoft Education products and access credentials for vetted third party products and services: pupils should only use the school Microsoft profile for communicating with known members of their community (as set out in the acceptable use policy that directs the approved use of electronic correspondence). Pupils should only create online accounts with the knowledge and permission of their parents or guardians acting in loco parentis, and teachers will moderate the use of such accounts, reporting inappropriate conduct, contact, and content through the reporting structure advised in the school safeguarding policy and other relevant policies including the IT and BYOD policies.

Compliance

The school will aim to meet the terms of its statutory obligation to provide internet service and supporting infrastructure for a superior computing education, with the highest standards of academic rigour, responsibility, and safety as its guiding principles.

The school's internet service will be designed for the use of pupils and personnel for educational purposes. Teachers and other personnel are expected to declare their intention to use the school's internet service for other purposes than education, including recreation and/or personal business. The internet service will include appropriate filtering, firewall and other security measures.

Children will be taught how to use the internet safely, responsibly and respectfully, in accordance with the school's acceptable use policy, which specifies in detail the necessary action dictated by exposure to inappropriate conduct, contact, or content.

Children will be taught to understand and respect copyright, ensuring that credit is given to the author(s) of media accessed and reproduced for educational purposes.

Children will be taught to assess and evaluate the appropriateness, quality, and reliability of information and media they access on the internet.

Health and safety

The computing resource provision follows school policy and prevailing law by undertaking regular health and safety assessments in the computer lab. Any written report is copied to the health and safety officer.

Health and safety issues in safer internet and computing include:

- Awareness of appropriate working conditions
- Awareness when using electrical machinery
- Avoidance of repetitive stain injury
- Awareness of correct posture
- Correct procedures for setting up and moving equipment

- Inappropriate conduct, contact, and content

Further to service levels discussed above, it is recommended that if any pupil, or employee, wishes to express concern over the appropriateness of any information or media accessed deliberately or inadvertently, they should report this to the designated safeguarding lead.

Data security

The School's IT Manager is Senior Information Risk Officer (SIRO), and ensures that users of the service know how to report any incidents during which data protection may have been compromised.

All following school stakeholders sign an acceptable use policy (AUP):

- employees
- governors
- pupils
- parents
- volunteers

The AUP clarifies the responsibility of users concerning data security, passwords, and access. The school follows COBIS guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the local authority or their partners, and publishes technical specifications for data security.

The school insists that any restricted material must be encrypted if the material is to be removed from the school and seeks to limit such data removal.

Use of portable electronic devices

Personal electronic devices belonging to employees, including mobile phones, will not be used for educational purposes during the school day. School mobile phones are available for telephone communication on behalf of the school.

Personal mobile phones must not be used during formal school time.

Personal mobile phones provided to children by parents or carers must be stored in the school office during school hours. **Pupils may not use personal mobile phones during school hours**.

Portable electronic devices such as digital cameras and tablet computers, which have been approved by the school for educational use and conform to standards set by the Bring Your Own Device (BYOD) policy, may be used with the permission of parents and personnel, and by pupils in Years 9 to 11. Photographs may only be taken with permission. Photographs or any other recordings of pupils may only be taken for educational purposes with the consent and knowledge of the parent(s) or guardian(s), and may only be taken on approved devices, an inventory of which is regularly updated.

Privacy

The school's formal and freely circulated contact details are published on the school website; they consist of the school's address and telephone number.

The personal information of any individual employee or pupil will not be published on the internet by the school, and all personnel must exercise vigilance to ensure that no such information is published, even if consent is perceived to have been given.

The executive principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate, and that any breach of privacy is investigated.

CCTV recordings for personnel and pupil safety will be retained by the school for 21 days and may only be disclosed without permission to the police as part of a criminal investigation.

Publication of electronic media

Photographs of pupils will be carefully selected; such photographs will not enable individual children to be identified.

No first or full names of children will be captioned with any photograph published on the website and the school will publish group photographs rather than photographs of individual children where possible. Photographs are published in accordance with signed agreements by parents and/or carers.

Photographs will only be taken on devices approved for such use by the school.

Photographs will not be taken with personal mobile phones, or any other personal electronic device and management will ensure that such activity is prohibited, unless authorised in writing for specific, exceptional cases.

Children's full names will not be published on the school website, nor will they be published on school blogs, forums, or wikis.

Photographs of adults working in (or visiting) the school will not be taken without consent.

Parents should be clearly informed of the school policy on media capture (including photography, audio recording and video recording) and publishing, both on school repositories (including the school website) and independent repositories.

Personal social media

The school will approve the use of specific, age-appropriate, social media services for educational purposes and pupils will use such services in accordance with the AUP, under the guidance of their teacher(s).

Parents will be reminded of prevailing international law regulating the collection of personal data from children under the age of 13 by social media service providers.

Teachers must not use personal social media to communicate with pupils, and should instead use approved digital communications services provided by the school, and only with the consent and knowledge of parents or guardians.

Personnel should not communicate with a pupil or ex-pupil though personal social media, unless the ex-pupil has reached the age of 18, and such communication is discouraged.

Teachers are obligated to report inappropriate conduct, contact, and content exhibited or shared on the internet by pupils, and such reports will be shared with parent or carers.

All adults working with children will be made aware of the school's safeguarding policy, which overrides this policy.

Social media at school

Personnel and persons acting on behalf of the school (volunteers and other adults who work with children in the school's interests) must comply with the terms of the AUP and the social media policy. Social media applications include, but are limited to, public applications such as open discussion forums and internal applications such as project blogs regardless of whether they are hosted on school networks or not. Where applications allow the posting

of messages online, users must understand that the right to freedom of expression is attached only to lawful conduct. The school expects that users of social media applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with prevailing law (including copyright law).

Safer internet at home

Many internet service providers offer tools to help parents administer a safer internet at home. However, it is not possible to guarantee complete protection from inappropriate content displayed on an electronic device at home or in public.

Parents are advised to explore:

- Google Safety Centre (https://safety.google/)
- Microsoft Family Safety (https://www.microsoft.com/about/family-safety/)
- UK Safer Internet Centre (https://www.saferinternet.org.uk/)

Pupils are instructed to share their experience of using the internet at home and at school (in accordance with their AUP) with their parents or carers and are given guidance on how to respond to inappropriate conduct, contact, and content.

At home, maintaining the standard set by the school's acceptable use policy will help further educate children in safe and responsible use of the internet during their leisure time, which should be consistent with their educational and personal interests. Certain websites of educational value are recommended by the school; these are communicated regularly to parents by teachers. The acceptable use policy is available to download from the school website, and a copy of any child's signed AUP may brought home by the child to share with their parents.

Disclaimer

The school will take all reasonable precautions to ensure that pupils, under supervision and with adequate instruction in sensible and intelligent use, will access appropriate and reliable media and information. However, due to the scale, scope, and nature of internet content, it is not possible to guarantee complete protection from inappropriate content displayed on an electronic device for which the school is responsible. Neither the school, nor any governing body may accept liability for damage or distress arising from exposure to inappropriate content.

While parents or carers are permitted to take personal photographs or recordings of their children on the school premises, the school may not accept responsibility for photographs taken by visitors to the school when these photographs have been taken in breach of this policy or prevailing laws governing privacy and consent. The school informs parents and other stakeholders, through this policy, of the rules governing the capture of media and recordings of children and vulnerable people.

If in doubt, a person wishing to take a photograph or recording of any child on the school premises should seek the permission of a representative of the school office.

The school will audit internet service provision annually to establish effective and rigorous implementation of this policy.

Acceptable use policy for the school

This acceptable use policy is written in clear, suitable, and appropriate language for both personnel and pupils. It does not exclusively restrict itself to the IT and computing domain but addresses copyright, privacy, responsibility, safety, and respect in both real and virtual contexts.

- In school, we will care for all our things.
- We will keep our gardens, grounds, spaces, rooms, and tools clean and tidy.
- We will use our tools properly and do our best learning with them.
- We will search for the things we want to learn about.
- We will respect the privacy of others and ask others to respect our privacy.
- We will protect our passwords, never sharing them.
- We will be ourselves, never pretending to be someone else.
- We will only say or write things on the internet we would be proud to say or write in public.
- We will not do mischief with files, services or other people's work.
- We will not waste paper or other resources.
- We will make our own things, and if we want to use someone else's things, we will ask them first.
- We will learn what intellectual property is, and we will always respect it.
- We will tell our teachers about the devices we are bringing to school.
- We will only communicate with people that have met our parents or teachers, and we will IMMEDIATELY tell our parents or carers about any requests for contact from strangers.
- We will ask our teacher if it is OK to communicate with famous people we have not met, and we will respect our teacher's decision.
- We will know that people we trust already know the important things about us, like our address and phone number, so we will NEVER write this information on the internet.
- We will be kind to each other and report any bullies or mean things we have seen or heard.
- We will care for the computer room, just as we would care for our school.
- We will learn about netiquette, and remain as polite online as we are offline.
- We will help our peers, teach them, and learn from them.
- We will remember that our teachers care about what we do with the world.
- We will recognise that our teachers can find out what we have been doing.
- We will accept that if we do not keep our promises, there will be penalties.
- We will try our best to be wonderful users of the world and the internet.
- We will remember safety, responsibility, and respect.

The rights afforded to our pupils ("we will search for things we want to learn about") in the AUP are derived from Article 13 of the UN Convention on the Rights of the Child (2013).

Social media policy

Scope

This policy governs the use of social media applications by all school stakeholders, including employees (and other adults working with pupils), governors, and pupils. These groups are referred to collectively as school representatives for brevity.

The requirements of this policy apply to all users of social media applications that are used for any school-related purpose and regardless of whether the school representatives are contributing in an official capacity to social media applications provided by external organisations.

Social media applications include, but are not limited to

- blogs;
- collaborative spaces such as Facebook and Instagram;
- media sharing services such as YouTube, and
- micro-blogging applications such as X.

Use

Use of social media applications at work for personal use is not permitted on the school's internet service. School representatives are permitted to use social media on their personal devices in a private environment.

- Social media applications must not be used to publish any content which may result in the actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages;
- be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- be used in an abusive or hateful manner;
- be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff;
- breach the school's misconduct, equal opportunities or bullying and harassment policies, nor
- be used to discuss (or advise on) any matter relating to school business.

Employees should not identify themselves as a representative of the school on any social media application or service, nor refer to the school by name, nor any pupil by name. Employees wishing to promote or support the school's mission, business, leisure, or charitable activities should do so through the school's official social media channels and may apply to the designated manager for publicity or social media communication, whether the executive principal, the bursar, or IT support personnel.

All school representatives must understand that information shared through social media applications, even if they are on private spaces, are subject to copyright, data protection, and freedom of information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

Pupil media approval

Parents or carers will sign and return a consent form at the start of each academic year. The consent form that authorises internet access for their child and it approves the use of specific services offered by the school.

The school will keep a record of all acceptable use policies and consent forms signed by parents, personnel, and pupils. The record will be managed by the school's IT support personnel.

The consent form may be downloaded from the school website.

5. Reporting and dealing with incidents

Complaints

Complaints of inappropriate conduct, contact, or content on the school's internet will be submitted to the designated safeguarding lead officer.

Complaints of inappropriate conduct, contact, or content on the school's internet by employees will be submitted to the head of education.

Complaints of inappropriate conduct, contact, or content on the school's internet by the head of education will be referred to the manager of human resources.

6. Enforcement of policy

Prevailing law

- Prevailing standards of protection and safety are set by the Department for Education in the September 2016 version of the document, *Keeping children safe in education: for schools and colleges*.
- Children are guaranteed the right to search for information using electronic devices by the United Nations Convention on the Rights of the Child (2013).
- The Children's Online Privacy Protection Act (COPPA) is a United States federal law, and applies to the online collection of personal information from children under 13 years of age. While children under the age 13 can legally give out personal information with their parents' permission, many websites ---

  particularly social media sites -- prohibit underage children from using their services altogether due to the cost and work involved in complying with the law. Therefore, most social media sites, especially those owned by US companies (Facebook and Twitter among others) do not permit children under 13 to apply to use their services. In keeping with policy, the school discourages the use of commercial social media by pupils.
- In England, teachers comply with the Teachers' Standards (2012).
- Children and vulnerable people are protected by the Safeguarding Vulnerable Groups Act (2006).
- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act (1998).

This policy will operate in conjunction with other school policies:

- Behaviour
- Anti-bullying
- Computing policy overview
- Computing education
- Computer science
- Digital literacy
- IT
- Bring Your Own Device
- Safeguarding and child protection
- Safer internet
- Blended learning
- Virtual classroom
- Data protection

Policy Prepared By:

Name: Mr. Raphael Sarker

Signature:

CEO	Head of Education
Mr Zied Ben Ghorbel	Ms Jacqueline Johnson
Date:	Date: 28/08/2025