THE ENGLISH COLLEGE DUBAI

PART OF iSP International Schools Partnership

Digital Safeguarding Policy
AY 2026-2027

AIM: (final result we are aiming to achieve)**:**

At The English College (**EC**), we want to ensure that staff, parents and students are committed to using the internet and other digital technologies to:

- Make learning more exciting and interactive.
- Make lessons more varied.
- Enable students to gain access to a wide variety of knowledge in a safe way.
- Raise educational standards.
- Prepare our students for using the internet safely outside of school and throughout their education.

This policy ensures that all digital use aligns with current UAE legislation, including the UAE Cybercrime Law (Federal Decree-Law No. 34 of 2021), UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021), and the UAE Child Digital Safety Law (Federal Decree-Law No. 26 of 2025).

RATIONALE: (The reason for which this policy has been written)

Wellbeing and achievement are at the heart of The English College so that we can all develop as life-long learners and take responsibility for ourselves and the community.

This Digital Safeguarding Policy is written for the context of The English College. It covers all aspects of online and offline activities and behaviour, including the use of devices that are both school owned and student/staff owned. The policy's primary intention is to safeguard students and members of staff at The English College and to ensure they maintain their own digital safeguarding beyond the school gates.

The English College has a duty of care under the Laws to assess and prevent possible harm to children and, therefore, this policy aligns with other policies at The English College, including:

- Safeguarding Policy
- EC Standards
- Acceptable Reasonable Use Policy
- Health and Safety Policy
- Anti-Bullying Policy

- Positive Behaviour Policy

GUIDELINES: (The principles/instructions/steps of the policy)

The field of digital safeguarding is constantly evolving with the pace of technological change. Schools need to manage the attendant risks actively and in a timely manner to achieve effective digital safeguarding. The change in terminology from E-Safety to digital safeguarding indicates a change in emphasis; away from the former's association with pure technology towards the latter's alignment with other areas of safe practice. Many of the issues that arise in digital safeguarding are behavioural and their management is no different from ensuring appropriate behaviour in any other area of school life or professional activity.

KEY ROLES AND RESPONSIBILITIES

The English College will have a Designated Digital Safeguarding Lead (DDSL) with overall responsibility for digital safeguarding at EC. The DDSL will:

- Create and update supporting documentation and resources and arrange training around Acceptable Use of Technology at EC.
- Monitor and review The English College safeguarding training and education for staff, parents and students alongside the school's Designated Safeguarding Lead and the IT department.
- Provide supported networks for hard-wired and, where applicable, mobile devices. Provide technical assistance for the systems that it supports via the IT Team
- Keep staff informed of updates, trends and developments that could have implications for student well-being and safety.
- Take an active role in supporting disclosures made that have a digital safeguarding concern.
- Undertaking appropriate training, such as CEOP Ambassador training, to acquire a detailed insight into current concerns and consequences of particular situations and actions; reporting of Incidents such as sexting to the school's DSL and Safeguarding Leads i.e The English College Safeguarding Team
- Having a solid pedagogical insight that can assess the learning benefits of any change when balanced with the associated potential digital safeguarding risks
- Should be trained in e-safety issues and applicable Laws, and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - Sharing of personal data
    - Access to illegal / inappropriate materials
    - Inappropriate on-line contact with adults / strangers
    - Potential or actual incidents of grooming
    - Cyberbullying
- Ensure members of staff are informed about lines of external support that are available, such as the Professionals' Online Safety Helpline (helpline@saferinternet.org.uk) operated by the UK Safer Internet Centre

- Monitor practice, develop and keep up-to-date the Digital Safeguarding Policy which must accurately reflect the requirements of The English College Digital Safeguarding Policy and the school's own practice;
- Develop, write and review ARUP (Acceptable Responsible use Policy) and ensure these are signed by children and parents where applicable;
- Ensure that the above documentation is filed for future reference if required;
- Ensure that any personal data that is processed by EC during the course of internet or online use at EC is carried out in accordance with EC's Privacy Notice
- Ensure there are clearly understood measures to deter and reform inappropriate behaviour for staff and students; This includes the use of inappropriate language, including racial/discriminatory language, this includes using incorrect spelling or emojis.
- Establish, monitor and maintain a Digital Safeguarding Log on My Concern in which all issues are recorded as they arise, together with a Digital Safeguarding Risk Assessment File detailing concerns and potential new development to show that risks have been appropriately considered and are periodically reviewed.
- Audit practice across the school and produce an action plan to improve the schools digital safeguarding provision using a self-evaluation framework such as SWGFL's 360 Safe (www.360safe.org.uk). Practice will be audited internally every year and externally every two years.
- Ensure that public communications on behalf of the school through digital channels, including social media, are appropriately managed and consistent with all applicable policies.
- Ensure that our digital safeguarding programme is taking place by monitoring weekly planning and ensuring there are Assemblies on E-Safety issues throughout the year in each Phase of the school
- Publish a half-termly digital safeguarding newsletter to parents via ISAMS with all the latest information regarding online safety.
- The DDSL must ensure that emerging risks such as AI misuse, deepfakes, anonymous accounts and online impersonation are regularly reviewed and addressed within the school's safeguarding framework.

The English College has Safeguarding Leads in each phase of the school to monitor, review and develop best practice.

It is expected that all members of the safeguarding team, including the DDSL, and all senior leaders across the Primary and Secondary schools are trained to a high level, equivalent to Safeguarding Level 3. The DDSL will also be a CEOP (Child Exploitation and Online Protection) Ambassador.

The DDSL alongside the Whole School Leadership Team (WSLT), must ensure Digital Safeguarding is given a suitably high priority and is considered within the school's development and improvement planning. Digital safeguarding logs, risk assessments and other documents must be available to the WSLT on request. All members of staff must be appropriately trained annually (and when a pressing development arises) in digital safeguarding by the schools Designated Digital Safeguarding Lead.

Key Responsibilities for IT Network Team

- Monitor that systems are put in place to reduce and, where possible, prevent inappropriate behaviour and the accessing of unacceptable content. This includes the use of inappropriate languages, including racial/discriminatory language, this includes using incorrect spelling or emojis.
- Manage and maintain different user profiles for web filtering to provide protection as appropriate and flexibly as required.
- Create monthly reports of the websites students and staff have tried to access that have been denied and share with the safeguarding team. The report will include the name, day, time, website url and the device used and be forwarded to the heads of school. Such reports shall be used and processed in accordance with the Laws, particularly the UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection (the **UAE DPL**).
- Ensure that all platforms used by staff and students are compliant with UAE data protection laws and that no unauthorised tools (including AI platforms) are used to process personal data.
- Conduct active testing to ensure that blocked content remains inaccessible.
- Monitor the selection of all web based services by members of staff to ensure use is consistent with the Term and conditions (including minimum age) and with all legal requirements (including the UAE DPL).
- Encourage appropriate and secure use of file storage locations and of encrypted memory sticks for the transportation of personal data, including in accordance with the UAE DPL.
- Ensure procedures are in place to prevent digital safeguarding decisions being taken by technical staff.
- Convey clear messages and employ workable measures to discourage users from connection to external networks whilst on school premises.
- Monitor the schools online profile and presence, including unofficial sites.

Staff Members' Key Responsibilities

- Act on all digital safeguarding issues promptly and in accordance with the school's Digital Safeguarding Policy and ARUP
- Ensure Students of Determination are provided with the skills and support via The Inclusion Team to safely navigate Distance Learning online
- Be diligent when digital safeguarding issues suggest child protection concern: follow child protection procedures immediately in these circumstances in line with Wadeema's Law (Federal Law No. 3 of 2016 on Child Rights) Article 2
- Work within the schools digital safeguarding measures and not attempt to compromise or circumvent those measures
- Protect professional boundaries by, for example, not giving students a member of staff's mobile number, not allowing a staff network log-in to be used by a student and not becoming friends with students on social media sites
- Be diligent in respect of data protection: use encrypted memory sticks whenever possible and ensure that data is always kept in authorised jurisdictions
- Staff must not:
    - Use personal devices or storage to hold sensitive student data

    - Upload data to AI tools or external platforms unless it has been fully anonymised, with no names, identifiers, or data combinations that could lead to the identification of a student.
- Select websites for school use only after reviewing Terms and Conditions, especially in regard to data protection compliance and minimum permitted age
- Seek advice from the school's Designated Digital Safeguarding Lead whenever necessary to discuss concerns, develop best practice and support students.
- Whilst we discourage one-to-one online meetings with students, if this is essential, a prior emailed consent of the student and parent is necessary and the meeting should be recorded.
- Should be trained in e-safety issues and applicable Laws, and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - Sharing of personal data in violation of the UAE DPL
    - Access to or posting of illegal / inappropriate materials in breach of the Laws, including the UAE Cybercrimes Law
    - Inappropriate on-line contact with adults / strangers
    - Potential or actual incidents of grooming
    - Cyberbullying
- Agree to an Acceptable Use Policy and The EC Standards and be aware of the responsibilities bestowed by each Agreement
- Staff must not upload student data, images, or personal information into AI tools or any unapproved external platforms.

Students' Key Responsibilities

- Work within the school's digital safeguarding measures and try not to compromise or bypass these measures.
- Know both how, and whom (DDSL and DSL need to be known to students) to report anything to, that could improve the digital safeguarding environment and the digital/online wellbeing of students,
- Respect personal privacy of others and keep their own personal data private, including photographs and passwords.
- Password guidance is a follows:
    - Change password from the preset versions.
    - Do not use an obvious secret questions e.g. Name of their school
    - Passwords should include at least 8 characters—the more characters, include a mixture of both uppercase and lowercase letters, a mixture of letters and numbers and the inclusion of at least one special character, e.g., ! @ # ?]
- Do not share any personal data or photographs of other students and staff or any text and images that contravenes the Laws, including the UAE DPL and the UAE Cybercrimes Law. Any publication or sharing of photographs of other individuals without the consent of that individual is a crime under the UAE Cybercrimes Law (Law No. 34 of 2021).
- The use of artificial intelligence to generate images or content that is inappropriate for the school setting constitutes a violation of digital safeguarding policies. For example, the creation of Deepfakes. Such use will be monitored and

may lead to disciplinary action as outlined in the school's Positive Behaviour Policy.
- Be aware of and contribute towards any support systems that encourage students to discuss digital safeguarding concerns they may have, including peer to peer support and opportunities to talk to members of staff.
- Behave in a healthy and positive manner towards digital technologies when engaging in online activities.
- When engaging in online activities being aware of the dangers which can arise from:
    - Sharing of personal data in breach of the Laws
    - Accessing or posting illegal / inappropriate materials, including posting private information relating to a person without their permission (which includes images and videos), spreading damaging news relating to a person (even if true), insulting religions and their rituals, posting offensive posts on online platforms or slandering public officials
    - Engaging in Inappropriate on-line contact with adults / strangers including the potential or actual incidents of grooming
    - Cyberbullying
- Read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of web services, especially with regard to the minimum age that some companies set for their websites in order to protect young people from risk.
- Do not create social media accounts which include The English College name and/or logo.
- Do not create any social media accounts under a name other than their own with the intention of using the anonymity inappropriately.
- Sign (digital) an appropriate Acceptable Responsible Use Policy and understand what the agreements mean.
- Students must not create, share or engage with anonymous or impersonation accounts that involve members of the school community.
- Students must not create or share AI-generated or edited content (including images, videos or audio) that involves other students or staff.
- Online behaviour outside of school, including social media activity, will be addressed where it impacts the school community.

Parents' Key Responsibilities

- Discuss the school's Acceptable Responsible Use Policy with their child(ren) and explain its implications at school and at home.
- Access support systems in school and via the Internet to develop appropriate awareness of how to protect their child.
- Talk through concerns about digital safeguarding with an appropriate member of staff as necessary.
- Know how and whom to report concerns to in order to improve the digital safeguarding environment and protect their child both at home and at school. (See above),
- Work with the digital safeguarding measures the school has in place.

- Respect digital safeguarding, cybercrime and data protection advice when sharing images, videos and text, especially personal data on social networking sites. Respect school passwords and encourage their child never to attempt to obtain or use another child's or adult's password.
- Refrain from posting anything online or on social media which can be seen to be defaming the school in any way. Note that the publication of insults or defamatory content is a crime under the UAE Cybercrimes Law.
- Whilst on the school site refrain from taking photos/videos, including during sporting matches and drama performances of any child other than their own. Under no circumstances should parents be sharing images of other children, or information that identifies other children, on social media. Note also that the publication or sharing of images or videos of other individuals without their consent is a crime under the UAE Cybercrimes Law.
- Encourage their child to read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of web services, especially with regard to the minimum age that some companies set for their websites in order to protect young people from risk.
- Online activities that are illegal in the UAE may be reported by the victim to the police, and we will cooperate fully with any police investigations. Parents also have the option to report to the police if their child has been a victim of an e-crime using digital technology, whether it occurred during or outside of school hours.
- In line with UAE Child Digital Safety Law (2025), parents are legally responsible for monitoring their child's online activity and ensuring appropriate safeguards (such as parental controls) are in place.
- Parents must ensure that their child uses age-appropriate platforms and follows safe online practices.

E SAFETY

Our school will endeavour to ensure the e-safety of all its members. It will use education, technology, accountability and responsibility as the key ways to achieve this. Within our school, all members of staff and pupils are responsible for e-safety, responsibilities for each group include:

Students E Safety Responsibilities

- Behave responsibly and appropriately when using communication technology including the internet and online behaviour platforms.
- Lock their screen if they leave their device, even just for a short period of time.
- Do not write down or share their passcode/password with anyone else in school.
- Use the school BYOD wifi network for gaining access to the internet; no access should be provided by the use of data plans.
- Irresponsible use may result in the loss of Network/Internet access.
- Copyright, intellectual property rights and the Laws must be respected.
- E-mail and posts on Google Classrooms should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.

- Users are responsible for e-mail they send and for contacts made. Anonymous messages, chain letters, are not permitted. "Spamming", cyber bullying and the use of chat rooms is not permitted.
- Access to sites containing illegal, offensive, pornographic, racially or religiously offensive material is not allowed and may be a crime under the UAE Cybercrimes Law
- Compromising or damaging the security or stability of the network is not allowed
- Pupils may only use approved e-mail accounts on the school system for school purposes.
- Students must immediately tell a teacher if they receive an offensive or inappropriate e-mail.
- Students must immediately tell a teacher if they receive communication from an unknown source. Students should be aware of the steps of grooming and be aware that people online are not always who they say they are.
- Students are responsible for all activities that are carried out under their school email/personal email. We will not be liable where their password or user name is used by someone else.
- Students agree to inform the DDSL of any unauthorised use of their password or user name of which they become aware. We have the right to disable any user account or password, whether chosen by themselves or allocated by us, at any time if we confirm any breach of code of conduct.
- When signing in to a public device with their school email and password make sure to log out afterwards - this includes Google Drive, Classroom and GMail.
- Do not share any personal data or photographs of other students or staff or any text and images that contravenes the Laws, including the UAE Cybercrimes Law and the UAE Copyright Law (Law No. 38 of 2021), notably:
    - *The "use of information network, electronic information system or information technology methods, for the purpose of breaching the privacy of a person or private or family life of individuals without consent, other than legally permitted, shall be sentenced to detention for a period of not less than (6) six months and/or to pay a fine of not less than (150,000) one hundred fifty thousand Dirhams and not more than (500,000) five hundred thousand Dirhams". This includes "Taking photographs of others at any public or private place or preparing, communicating, exposing, copying or keeping electronic images thereof". Article 44 of the UAE Cyber Crime Law.*
    - *It is not "permissible for anyone with whom it has been agreed to take a photograph of another or sound or visual recording, in any way whatsoever, to keep, publish, exhibit, or distribute the original or Reproductions thereof without the permission of that person, unless otherwise agreed upon". Article 45 of the UAE Copyright Law.*
- Behave in a healthy and positive manner towards digital technologies when engaging in online activities.
- Read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of Web Services (for example - Google Terms and Conditions of web services here), especially with regard to the minimum age that some companies set for their websites in order to protect young people from risk.

- Sign the ARUP (Acceptable Responsible use Policy) and understand what the agreement means.

Reporting Process for Students - all should be reported on as soon as possible and as a maximum timeframe, within 48 hours.

- Report anything unusual or inappropriate during teaching lessons, either in person or online, to the class teacher or form tutor or another trusted adult within the school
- Report to class teacher or form tutor or another trusted adult within the school
    - If when accessing the device or computer, the student sees any obscene or inappropriate pop ups, cookies or accidentally gains access to inappropriate websites
- Report any inappropriate behaviours by peers when engaged in online lessons or engaged in online learning, and report it to the class teacher or form tutor or another trusted adult within the school. This includes the use of inappropriate language, including racial/discriminatory language, this includes using incorrect spelling or emojis.
- Inform the network team of any unauthorised use of their password or user name of which they become aware as soon as possible.
- Primary - Tell a trusted adult if the students sees anything that makes them uncomfortable or scared when online using their school online account

Teaching Staff E Safety Responsibilities

- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- They report any suspected misuse or problems the students encounter to the heads of year and the network team.
- E-safety issues are embedded in all aspects of the curriculum and other activities They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed and in accordance with the Laws) and implement current policies with regard to these devices. In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use.
- Respect personal privacy of others, including any processing of personal data of students or parents, in accordance with the Laws, and keep their own personal data private, including photographs and passwords.
- Do not share any personal data or photographs of students or staff or any text and images that contravenes the Laws, including the UAE Cybercrimes Law and the UAE Copyright Law (Law No. 38 of 2021), notably:,
    - *The "use of information network, electronic information system or information technology methods, for the purpose of breaching the privacy of a person or private or family life of individuals without consent, other than legally permitted, shall be sentenced to detention for a period of not less than (6) six months and/or to pay a fine of not less than (150,000) one hundred fifty thousand Dirhams and not more than (500,000) five hundred thousand Dirhams". This includes "Taking photographs of others at any public or private*

place or preparing, communicating, exposing, copying or keeping electronic images thereof". Article 44 of the UAE Cyber Crime Law.
    - *It is not "permissible for anyone with whom it has been agreed to take a photograph of another or sound or visual recording, in any way whatsoever, to keep, publish, exhibit, or distribute the original or Reproductions thereof without the permission of that person, unless otherwise agreed upon". Article 45 of the UAE Copyright Law.*
- Behave in a healthy and positive manner towards digital technologies when engaging in online activities.
- Read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of Web Services (for example - Google Terms and Conditions of web services here)
- Sign the ARUP (Acceptable Responsible use Policy) and understand what the agreement means.
- At least three members of staff should have access to any school-authorised social media account, including a member of the school leadership team and the Marketing and Communications Manager.
- In relation to staff members personal social media accounts:
    - Posts should be positive and professional. Staff need to think twice before posting, and check posts with a trusted colleague to help with tone and editing. Staff should not post inappropriate or illegal content: such content may expose staff to criminal sanctions under the UAE Cybercrime Law.
    - Confidential, proprietary, personal or privileged information about other staff, students, parents/carers, or school projects, policies or finances should never be posted or published.
    - Do not interact with students or parents on social media platforms.
    - It is recommended that accounts should be set to private and deny friend or message requests from current and past students.
    - Staff in doubt about professional social media use should ask for guidance from a member of WSLT or the DDSL.

Reporting Process for Teachers

All should be reported on as soon as possible and as a maximum timeframe, within 24 hours.

- Report anything unusual or inappropriate when teaching lessons, either in person or online. If the issue is related to behaviour, record it on ClassCharts or Class Dojo; if the behaviour is related to safeguarding, log it on MyConcern.
- Report anything unusual or inappropriate to the I.T Network Team if when accessing their computer, any obscene or inappropriate pop ups, cookies or inadvertent access to inappropriate websites occurs
- If approached by a student or parent/carer with concerns about inappropriate content or misconduct on school social media, staff must report to their WSLT link and the DDSL.
- Escalation process:
    - Staff logs concern (MyConcern/ClassCharts/ISAMs)
    - DSL/DDSL reviews incident
    - WSLT involvement where required

- Referral to external authorities (including UAE Cybercrime Unit) where appropriate

Cyberbullying

Cyberbullying means bullying by electronic means which occurs through the use of technology, including computers or other electronic devices, social networks, text messaging, instant messaging, websites, or e-mail. The consequences are both emotional and educational.

Cyberbullying includes:

- Harassment via digital platforms
- Sharing harmful or inappropriate content
- creation of anonymous accounts, impersonation, and AI-generated content.

Cyberbullying differs from other methods of bullying and has several key differences:

- Cyberbullying can happen any time and any place and for many young people home is no longer a safe place from bullying.
- Online communication between young people is often hidden from adults and free from supervision.
- The anonymity the internet offers has consequences such as the targets don't know the identity of their bullies which can lead to the "victim" refraining from communicating with all others.
- Youngsters who post online are not as responsible for their actions as they should be, usually through ignorance of the permanence of the post. They are usually not immediately confronted with the consequences of their actions as they might otherwise, which makes them less "fearful" of being punished.
- Digital content can be shared and seen by a large audience almost instantly and is almost impossible to delete permanently.
- Young people are often fearful of reporting incidents, as they fear the adults will take away their devices.

Students cyberbullying responsibilities

- Students must know both how, and whom to report anything to, that could improve the digital safeguarding environment and the digital/online wellbeing of students
- Pupils are able to explain what "Cyberbullying" is and can spot incidents whether they are relating to themself or others.
- Pupils are aware of the "go to" people within the school and are encouraged to report any cyberbullying they experience:
  - Classroom Teacher/Form Tutor
  - Counsellor
  - Senior leaders
- Students are educated on the dangers of technologies and online communication through the school's pastoral programme, as well as the consequences of posting insulting and defamatory information online which is a crime under the UAE Cybercrimes Law. This includes; educational videos, assemblies and tutor time activities.
- Pupils are informed of appropriate online behaviours and what Cyberbullying is within these videos.
- Students must not engage with or promote anonymous or harmful accounts**.**

Reporting Process for Students - all should be reported on as soon as possible and as a maximum timeframe, within 48 hours.

- Report anything unusual or inappropriate when teaching lessons, either in person or online, to the class teacher or form tutor or another trusted adult within the school
- Report to class teacher or form tutor or another trusted adult within the school
    - If when accessing the device or computer, the student sees any obscene or inappropriate pop ups, cookies or accidentally gains access to inappropriate websites
- Report any inappropriate behaviours by peers when engaged in online lessons or engaged in online learning, and report it to the class teacher or form tutor or another trusted adult within the school. This includes the use of inappropriate language, including racial/discriminatory language, this includes using incorrect spelling or emojis.
- Primary - Tell a trusted adult if the students sees anything that makes them uncomfortable or scared when online using their school online account

Staff cyberbullying responsibilities

- Staff must be aware of how to spot incidents of Cyberbullying within the school environment.
- Staff who were informed of any inappropriate online behaviours are to add to class charts if this is a behaviour related issue. If there are any safeguarding concerns, then it should **also** be recorded following the school's safeguarding reporting procedures.
- Safeguarding staff including the DDSL Staff will act to deal with the cyberbullying issue. This might include a conversation with the child, a conversation with the perpetrator, safeguarding conversations, contact with home, contact with the counsellor etc. The safeguarding and positive behaviour policies will guide decisions made and actions taken.
- Each incident will be dealt with on a case by case, consulting the positive behaviour policy. Both the "Bully" as well as the "Victim" will be offered emotional support and guidance.

Reporting Process for Teachers - all should be reported on as soon as possible and as a maximum timeframe, within 24 hours.

- Report anything unusual or inappropriate when teaching lessons, either in person or online. If the issue is related to behaviour, record it on ClassCharts or Class Dojo; if the behaviour is related to safeguarding, log it on My Concern.
- Report any inappropriate student behaviours when teaching online lessons or engaged in online learning, and report it to the relevant SLT member of that year group.

Artificial Intelligence (AI) and emerging technologies

The English College recognises the increasing use of Artificial Intelligence (AI) in education and society. While AI can enhance learning, it also presents safeguarding, ethical and academic risks.

Students must:

- Use AI tools responsibly and for appropriate educational purposes only
- Not submit AI-generated work as their own
- Not use AI to create harmful, misleading or inappropriate content

Staff must:

- Not upload personal or sensitive student data into AI tools or external platforms
- Use AI in line with professional and ethical expectations

The creation, sharing or possession of AI-generated or manipulated content (including deepfakes) involving members of the school community is strictly prohibited and will be treated as a serious safeguarding concern.
Misuse of AI may result in disciplinary action and/or referral to external authorities in line with UAE law.

Bring your own device

At The English College we are dedicated to a learning environment that gives access to appropriate technology in order to enhance learning, unlock potential and connect students both locally and globally.

The use of BYOD supports contemporary learning skills including:

- Accessing, filtering and processing information
- Planning and organising
- Making choices and decisions
- Problem Solving
- Communicating
- Being creative and innovative
- Risk taking and overcoming challenges.

BYOD applies to any device that is not school owned or supplied and is used to access the school network. The purpose of this part of the policy is to establish clear guidelines and procedures when students use their own devices in school, to ensure safe use and the integrity of the EC network.

Recommended devices:

Year Group	Preferred device
4-6	Chromebook, iPad
6-9	Laptop, iPad
10-13	Laptop, Macbook

Students may be required to download apps to suit their learning situation in the classroom, this may also include a Mobile Device Management software.

Students in Years 7-12 are only allowed to bring a phone into school after purchasing and using the Yondr pouch. Year 13 students may bring their phone into school and can use it on the third floor. Please refer to the Digital Device Policy 2026-27.

By bringing a personal device to be used for school work, the student agrees that the Digital Safeguarding Lead/leadership team may inspect the contents of files, photos, chats and social media use during school hours. This inspection will only occur in extreme cases to support relevant investigations, aligning with the school's commitment to maintaining a safe educational environment.

Confiscating and searching students' mobile phones or electronic devices

A student's personal device may only be searched when necessary for a safeguarding or behavioural investigation. Only the Principal or Head of School may authorise and conduct the search, with the DSL/DDSL present as a witness.

Before any search, the student and their parent(s)/carer(s) must be informed of what is being looked for and why. Agreement to proceed must be obtained from both the student and their parent(s)/carer(s). This discussion must be documented and signed by the student, the DSL, Principal or Head of School using the student device search form.

If either party refuses, the search will not proceed; if essential to preserve evidence, the matter will be immediately referred to the relevant authorities.

Any search must be strictly limited to the specific content required. The school will not access or copy unnecessary personal data, browse unrelated material, force password disclosure, or forward/store indecent images.

The use of VPNs to bypass restrictions is prohibited and may result in disciplinary action.

The use of devices to create or distribute harmful, inappropriate or AI-generated content involving others is strictly prohibited.

Technical Support
All students will be given the necessary help and guidance to set up passwords and access the internet, however, due to the large number of devices in the school, maintenance and technical support is the responsibility of the user.

Restrictions

- The use of a personal device in the school is for instructional use only and at the teacher's discretion.
- Primary school students are not permitted to use devices outside of lesson times.
- Secondary School students (years 7 to 11) are not permitted to use devices outside of lesson times. However, during lunchtime, students can go to the library and use their device for work purposes if supervised by the librarian.
- Sixth form students can use their device in the designated areas during their non-contact time.

Expectations

- Students are responsible for the safety, security loss or damage of their device. The school cannot be held responsible for student devices.
- Devices should only be used for learning purposes, as instructed by a teacher.
- Using the device to disrupt the learning of their peers will not be tolerated.
- Using the device to disrupt the teaching of a lesson will not be tolerated.

- Negative or disruptive conversations or comments that undermine or detract from learning may result in disciplinary action in line with the school's behaviour policies.
- Users must power off and put away personal devices if directed to do so by teachers or school administrators.
- Users should practice caution when allowing others to access their personal device. All liabilities remain with the user.
- All devices need to be fully charged when students arrive at school, however the student must also bring their charger just in case.
- Students can only connect to the internet via the school WIFI.
- The use of a device to take photos or videos without consent (staff or students), or to threaten the security or well-being of others, will result in disciplinary procedures. Note that such action may also be a crime under the UAE Cybercrimes Law.
- Students are not permitted to contact home through email, chat or any other medium during school hours without the permission of SLT or WSLT.
- The deliberate attempt to access inappropriate or offensive online content, as deemed by UAE guidelines, will result in disciplinary procedures.
- The use of a VPN to access banned websites/apps/games is prohibited as stated by applicable Laws. Students being found using a VPN will have the Positive Behaviour Policy applied to them and their device confiscated.

Personal data

- If EC has access, or is provided access, to personal data on the devices or its systems at any time, it will ensure that any processing of such personal data is carried out in accordance with its Privacy Notice.

School Community Digital Safeguarding

- The English College recognises the need for the safeguarding and digital wellbeing of members of staff by, for example, not publishing any of their personal details (including photos) online without consent.
- The English College does not require staff to use personal mobile phones to communicate with parents or students at any time:
    - The English College will provide staff with school-owned devices that can be used whenever on-site communication is needed.
- The English College evaluates and conducts risk assessments of new technologies to ensure that the anticipated educational benefits justify any potential digital safeguarding risks that might be identified, including likely misuse of the technologies.
- The English College ensures that an outline of the school's approach to digital safeguarding, including responsible use of technologies and appropriate technology based behaviour is communicated to all stakeholders.
- The English College also ensures that all children are aware of their responsibilities and regularly updated about digital issues in a meaningful and engaging manner.
- Equally, parents and carers will be made aware of their Digital Safeguarding responsibilities via The Parent Handbook and regularly updated about digital

safeguarding issues at an appropriate level in newsletters and that appropriate content is found on the school website for parents to access.

Photography and Consent - Please refer to the Digital Device Policy 2026-27

E Teaching

During the COVID-19 lockdown in 2020 we established a successful E Teaching approach (highlighted in the Teaching and Learning Policy). If something similar was to occur in the future here are the expectations of our community.

E Teaching expectations

Leadership

The Leadership at The English College, will exemplify and set the expectations for our learning community. The Head of Schools and Head of Faculties will be responsible from a whole school approach, in the terms of policy and accountability.

The following are other expectations of the leadership team at The English College:

- Leaders will be first responders to any administrative need from staff, students and parents.
- Leaders are to create, monitor and alter plans for remote learning. This can include careful curriculum modification to meet the needs of the Department/Faculty Leaders and progression for the next year level.
- Monitor assessment practices and rigorous evaluation of data to ensure data adapted interventions are appropriate.
- Devise strategies to ensure active participation from the students.
- Communicate the Distance Learning Plan to the school community.
- Monitor staff and student attendance and follow up regular absences to ensure staff and students are effectively engaged.
- Support with any technical issues that may arise with the online platforms being used.

Heads of Faculty/Year Group Lead for Primary

The responsibility for E Teaching is with every teacher in school. It is also therefore the responsibility of the HOF to monitor and ensure high standards are being met with the quantity and quality. Other expectations include:

- Communicate regularly with assigned teachers to support planning, facilitation of learning opportunities, lessons and creation of assessment tools.
- Provide teachers within the department with useful links, apps and alternate strategies as well as troubleshoot and offer technical support wherever needed.
- Collaborate with team members or departments to design distance learning experiences during scheduled or agreed upon collaborative planning times.
- Follow other responsibilities assigned to the leaders, as mentioned above.

Classroom Teacher

Teachers at The English College are expected to honour the school's high expectations for professionalism and conduct while delivering engaging and meaningful distance

learning to promote and align E Teaching strategies, the following steps are required by all teachers for all tasks:

- A Google classroom must be set up for every class and tutor group.
- Every student from the class should receive an invite from the teacher
- Department lead (in some cases another member of the department) should also be assigned as a teacher to each Google classroom.
- A Google meet code should be created for the classroom and be visible in the banner of the classroom
- Google classroom is to be used for uploading materials, however teachers may use it for a lot more e.g. collecting in work.
- If students are accessing a lesson via distance learning, the teacher is required to turn on their camera, mic and present their screen.
- Attendance will be taken during the first 10 minutes of every lesson and logged through iSAMs.
- Teachers should be available to students and colleagues during regular working hours
- Communicate curriculum expectations to students and deliver lessons as per the plan.
- Provide Assessments / Feedback as per curriculum expectations to support students' learning.
- The method of E Teaching is not prescribed, it is down to the teachers professional knowledge. Apart from the use of Google Classroom and Google Meet
- E Teaching should be in line with the Teaching and Learning Policy and The Curriculum Policy

Expectations of students accessing E Teaching:

- Students will still follow the Positive Behaviour Policy and Anti Bullying Policy
- The same high expectations and rigour will be placed on the students as normal classroom lessons
- Students inviting people from outside of The English College is strictly prohibited. An outside person gaining access to our online platforms will be dealt with as a police matter.
- Attainment and progress that is achieved through E Teaching will be recorded and reported on just as does classroom teaching
- Students must log into the Google meet from a distraction-free, quiet environment.
- Students will keep audio on mute until you want to speak. This will help limit the background noise.
- Students are not required to turn on their camera when at home. This is because a live feed into a students home/bedroom is not always appropriate. However, a teacher seeing the student may be vital to the lesson, if so the teacher will make students aware of this in advance.
- If they wish to speak or answer a question, use of the "Raise Hand" feature is recommended before unmuting after being called on.
- In case they are not comfortable answering the teacher led question on audio, they may write the answer in the chat box.
- Upload work/assessments/homework on time and to their usual in class standard.
- For KS 1 it is expected that parents are present in the room whilst on any kind of video call

- The recording, screenshotting or sharing of online lessons, images or content without permission is strictly prohibited and may constitute a breach of UAE law.
- Any misuse of online learning platforms, including capturing or distributing content, will be treated as a safeguarding concern.

APPENDICES (Relevant links to other policies or documents)

- The EC Standards
- Safeguarding Policy
- Acceptable Responsible Use Policy
- Anti-Bullying Policy
- Health and Safety Policy
- Teaching and Learning Policy
- Positive Behaviour Policy
- IT Policy
- Privacy Notice
- Digital Device Policy

Useful weblinks

1. Get Safe Online | www.getsafeonline.org/

One of the UK's leading source of unbiased, factual and easy-to-understand information on online safety.

2. Facebook Family Sharing Centre | www.facebook.com/safety

Learn about your account settings, safety best practices and more.

3. Internet Matters | www.internetmatters.org/

A not-for-profit organisation working with online safety experts to bring you all the information you need to keep your children safe online.

4. NSPCC Net Aware | www.net-aware.org.uk/networks/?order=-popularity#

Joint forces with O2 to help parents explore and understand online life as kids know it.

5. BBC Webwise | www.bbc.co.uk/webwise/0/

All round advice regarding online safety for young people.

6. UK Safer Internet Centre | www.saferinternet.org.uk/

The UK Safer Internet Centre, where you can find e-safety tips, advice and resources to help children and young people stay safe on the internet.

7. Tiger Mobiles | www.tigermobiles.com/2015/05/how-to-protect-your-children-on-their-smartphone/

A guide showing how to protect your children on their smartphone.

8. National Trading Standards | www.tradingstandardsecrime.org.uk/dont-fall-for-the-in-app-purchase-trap/

Advice and stats on in-app purchasing.

9. Think U Know | www.thinkuknow.co.uk/parents/

Advice and what to do if you have a concern.

10. Back to School Net Aware | https://www.net-aware.org.uk/news/back-to-school/

How to help your child stay safe online when school starts again.

11. Getting Naked Online | https://www.internetmatters.org/wp-content/

The dangers of getting naked online and sexting.

12. Cyber safety and digital security | https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

Cyber safety and digital security are serious issues in the UAE. Read how the UAE is protecting its citizens and residents in this field and reinforcing digital trust.

POLICY REVIEW HISTORY:

The Whole School Leadership Team monitors any Digital Safeguarding Concerns in order to ensure that all issues are handled properly.

Historical Record				
Revision No.	Date	Brief Description of Change	Approved by	Next Review:
0	1 May 2021	New Policy	Principal	June 2022
1	1/7/2022	Update		

2	04/01/2023	Update to Law references	WSLT	June 2023
3	08/06/2023	Reviewed and updated	WSLT	June 2024
4	02.07.2024	Reviewed and updated	WSLT	June 2025
5	09.06.2025	Reviewed, added about Yondr and more on photo consent	WSLT	June 2026
6	04.01.26	To align with ISP update regarding permissions needed for searching a device.	WSLT	June 2026
7	01/07/2026	Updated	WSLT	July 2027