THE ENGLISH COLLEGE
DUBAI

Digital Safeguarding Policy 2021-2022

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

At The English College, we 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.

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

Well-being 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 Law to assess and prevent possible harm to children and, therefore, this policy aligns with The English College **Safeguarding Policy**; **EC Code of Professional Practice**; **Acceptable Reasonable Use Policy**: **Health and Safety Policy**; **Anti-Bullying 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.

The Digital Safeguarding Policy is made up of the following sections:
E Safety
Bring your own device
E Teaching

E Safety

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 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 the 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.

Safeguarding steps for online interaction for students while being present at school:

1. Students are educated on the dangers of technologies and online communication.
2. The school has an online firewall system that filters all content, supported also by Google Safe Browsing.

3. Know both how, and whom to report anything to, that could improve the digital safeguarding environment and the digital/online wellbeing of students
4. Respect personal privacy and keep their own personal information private, including photographs and passwords.
5. Do not share any personal information or photographs of other students or any text and images that contravenes UAE laws,
   "using a visual device to invade the privacy of a third party by capturing their picture or transferring, copying, or keeping those pictures is a crime punishable by at least six months improsnment and a fine of up to AED 500,00" Article 21 of the UAE Cyber Crime Law.
6. Behave in a healthy and positive manner towards digital technologies when engaging in online activities.
7. 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 .
8. Sign the ARUP (Acceptable Responsible use Policy) and understand what the agreements mean,
9. Staff act on all digital safeguarding issues promptly and in accordance with the school's Digital Safeguarding Policy.
10. Pupils are informed of what "Cyberbullying" includes.
11. Pupils are informed of the "go to" people within the school and are encouraged to report any cyberbullying they experience:

    - Classroom Teacher/Form Tutor
    - Counsellor
    - Deputy Heads and Heads of School

Safeguarding steps for online interaction for students while in the home environment:

1. For KS 1 it is expected that parents are present in the room whilst on any kind of video call
2. 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 .
3. Remind parents of their obligations around the use of social media in the home environment.
4. Students are educated on the dangers of technologies and online communication through the school's pastoral programme. This includes; educational videos, assemblies and tutor time activities.
5. Pupils are informed of appropriate online behaviours and what Cyberbullying is within these videos.
6. Pupils are encouraged to report any incidents of Cyberbullying or incidents to their 'go to' adult or directly to their teacher/Deputy Head of Phase by sending an email with or without parental support.
7. Personnel 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.

8. 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.
9. 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 class charts; if the behaviour is related to safeguarding, inform the safeguarding team. There is the option to notify the form tutor or member of ESLT in addition.
- Report anything unusual or inappropriate to the I.T Network Team if when accessing your computer, any obscene or inappropriate pop ups, cookies or inadvertent access to inappropriate websites occurs
- Report any inappropriate student behaviours when teaching online lessons or engaged in online learning, and report it to the relevant ESLT member of that year group

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
- Primary - Tell a trusted adult if the students sees anything that makes them uncomfortable or scared when online using their school online account

Key Roles and Responsibilities

The English College will have a Designated Digital Safeguarding Officer (DDSO) with overall responsibility for this area to offer all areas of the school with expert advice, guidance and recommendations. He/She will:

1. Create and update supporting documentation and resources and arrange training around Acceptable Use of Technology at EC.
2. Monitor and review The English College safeguarding delivery alongside the school's Designated Safeguarding Lead and the IT department.
3. Provide supported networks for hard-wired and, where applicable, mobile devices. Provide technical assistance for the systems that it supports via the IT Team
4. Keep staff informed of updates, trends and developments that could have implications for student well-being and safety.

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

It is expected that the identified individuals are trained to a high level, equivalent to Safeguarding Level 3 and / or CEOP (Child Exploitation and Online Protection) Ambassador.

The DDSO alongside the Senior Leadership Team (SLT), 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 SLT 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 Officer.

School Designated Digital Safeguarding Officer Key Responsibilities include:

- Undertaking appropriate training, such as CEOP Ambassador, 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
- Attend relevant update training and support sessions to update staff on concerns and best practices
- 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
- Challenge and support members of staff to develop their awareness of and teaching about digital safeguarding
- 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 The EC Professional Professional Code of Practice has a Digital Safeguarding section;
- Ensure there are clearly understood measures to deter and reform inappropriate behaviour for staff and students;
- Establish, monitor and maintain a Digital Safeguarding Log in which are recorded all issues 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).
- Ensure that public communications on behalf of the school through digital channels, including social media, are appropriately managed and consistent with all applicable policies.
- Brief staff regularly on digital safeguarding developments.
- 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

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
- Manage and maintain different user profiles for web filtering to provide protection as appropriate and flexibly as required.
- 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 (UAE Data Protection Law)
- Encourage appropriate use of file storage locations and of encrypted memory sticks for the transportation of personal data.
- 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 all students have equal access to Distance Learning
- Ensure Students of Determination have appropriate support in Distance Learning, including one to one engagement and small group work for interaction that is supported by parents, teachers and learning support assistants.
- 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 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
- 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.
- Report anything unusual or inappropriate when teaching online lessons or engaged in online learning, and report it to the relevant ESLT member of that year group.
- Report any inappropriate student attire when engaged in online live lessons and ask the student to turn off their camera and report it to the relevant ESLT member.
- 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.
- Sign an Acceptable Use Policy and The English College Code of Professional Practice and be aware of the responsibilities bestowed by each Agreement

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 (DDSO 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 and keep their own personal information 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 information or photographs of other students or any text and images that contravenes UAE laws,
- 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.
- 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 .
- Sign (digital) an appropriate Acceptable Responsible Use Policy and understand what the agreements mean,

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 and data protection advice when sharing images, videos and text, especially personal information 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.
- 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.

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.

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
3-5	Chromebook, iPad
6-9	Chromebook, iPad
10-13	Chromebook, 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 7-11 are allowed to bring a mobile phone to school but it must not be heard or seen throughout the school day, unless they are instructed by their teacher. Therefore, if your child doesn't have a device to use in lessons, a phone can be used (however a tablet is preferred). Students in Years 7-11 can use their phone after school, but only in the designated areas: in reception, on the netball court or outside the front of the school.

Sixth Form students are welcome to bring their phones to school and can use them anytime in the designated areas; common room and outdoor study spaces (as well as lessons when instructed by their teacher.

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 others conversation 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 without consent, or to threaten the security or well-being of others, will result in disciplinary procedures.
- Students are not permitted to email home in school hours.
- 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 UAE law.

E Teaching

As the world moves forward more and more of what we do is now online. This was of course heightened during the previous COVID lockdown. However, E Teaching does offer great advantages to the students and staff, as well as helping to prepare students for the

working world, which is becoming increasingly digital. While staff have been finding that E Teaching Methods have enhanced their classroom, saved time and further developed the students' experience.

E learning is defined as 'teaching conducted via electronic media, typically on the internet". Therefore E Teaching is not solely related to a distance learning situation, it can be for any task, which can be completed with teachers and students present in the same room. This policy is of course highly related to **Teaching and Learning Policy**.

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:

1. Leaders will be first responders to any administrative need from staff, students and parents.
2. 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.
3. Monitor assessment practices and rigorous evaluation of data to ensure data adapted interventions are appropriate.
4. Devise strategies to ensure active participation from the students.
5. Communicate the Distance Learning Plan to the school community.
6. Monitor staff and student attendance and follow up regular absences to ensure staff and students are effectively engaged.
7. Support with any technical issues that may arise with the online platforms being used.

Heads of Faculty/Key stage 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:

1. Communicate regularly with assigned teachers to support planning, facilitation of learning opportunities, lessons and creation of assessment tools.
2. Provide teachers within the department with useful links, apps and alternate strategies as well as troubleshoot and offer technical support wherever needed.
3. Collaborate with team members or departments to design distance learning experiences during scheduled or agreed upon collaborative planning times.
4. 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:

1. A Google classroom must be set up for every class and tutor group.
2. Every student from the class should receive an invite from the teacher
3. Department lead (in some cases another member of the department) should also be assigned as a teacher to each Google classroom.
4. A Google meet code should be created for the classroom and be visible in the banner of the classroom
5. Google classroom is to be used for uploading materials, however teachers may use it for a lot more e.g. collecting in work.
6. If students are accessing a lesson via distance learning, the teacher is required to turn on their camera, mic and present their screen.
7. Attendance will be taken during the first 10minutes of every lesson and logged through iSAMs.
8. Teachers should be available to students and colleagues during regular working hours
9. Communicate curriculum expectations to students and deliver lessons as per the plan.
10. Provide Assessments / Feedback as per curriculum expectations to support students' learning.
11. 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
12. E Teaching should be inline with the Teaching and Learning Policy and The Curriculum Policy

Expectations of students accessing E Teaching

1. Students will still follow the Positive Behaviour Policy and Anti Bullying Policy
2. The same high expectations and rigour will be placed on the students as normal classroom lessons
3. 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.
4. Attainment and progress that is achieved through E Teaching will be recorded and reported on just as does classroom teaching
5. Students must log into the Google meet from a distraction-free, quiet environment.
6. Students will keep audio on mute until you want to speak. This will help limit the background noise.
7. 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.

8. If they wish to speak or answer a question, use of the "Raise Hand" feature is recommended before unmuting after being called on.
9. In case they are not comfortable answering the teacher led question on audio, they may write the answer in the chat box.
10. Upload work/assessments/homework on time and to their usual in class standard.

APPENDICES (Relevant links to other policies or documents)

- The EC Professional Code of Conduct.
- Safeguarding Policy
- Acceptable reUse Policy
- Anti-Bullying Policy
- Health and Safety Policy
- Teaching and Learning Policy

POLICY REVIEW HISTORY:

The Senior 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		

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.