THE ENGLISH COLLEGE

DUBAI

Digital Safeguarding Policy 2020/21

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 (E-Safety) 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**; **The EC Professional Code of Conduct**; **Health and Safety Policy**; **The Bring Your Own Device Policy**; **Acceptable I.T Usage Policy for Staff** and **Anti-Bullying Policy**.

The field of digital safeguarding, also known as E-Safety, 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.

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 safety system that filters all content. Students cannot access other platforms on the school browser.
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,
6. 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.
7. Behave in a healthy and positive manner towards digital technologies when engaging in online activities.

8. 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 .
9. Sign an appropriate BYOD and Acceptable Use Policy and understand what the agreements mean,
10. Staff act on all digital safeguarding issues promptly and in accordance with the school's Digital Safeguarding Policy.
11. Pupils are informed of what "Cyberbullying" includes.
12. 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. The school has an online safety system that filters all content. Students cannot access other platforms on the school browser.
2. For KS 1 it is expected that parents are present in the room whilst on any kind of video call
3. 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 .
4. Parent consent for all social media usage during this time is checked - relates to forms signed when joining school.
5. Pupils are educated on the dangers of technologies and online communication through "E-Safety Videos" which are posted on learning platforms for all pupils to see. Virtual Assemblies on E-safety will regularly support the school community.
6. Pupils are informed of appropriate online behaviours and what Cyberbullying is within these videos.
7. 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.
8. Personnel who were informed of any inappropriate online behaviours are to email the complaint to the Digital Safeguarding Officer (DSO), and their Deputy Head of School to investigate, to ensure it is recorded and evidence can be collected if need be
9. Students are invited for an online GoogleMeet session or face to face meeting with their class teacher, Deputy Head of Phase and are given both the opportunity to share their experiences, and are given the "tools" to handle their emotions.
10. Should the "Cyberbullying" continue, the students in question, if known, will be reported to the relevant Head of School (also Safeguarding Officer for their phase) who will then deal with the incident.
11. Each incident will be dealt with on a case by case.
    Depending on the severity - the consequences can vary from an informal warning to students, a recorded official warning to students including parents and online learning/internal/external suspension for repeated offences.

Both the “Bully” as well as the “Victim” are offered emotional support and guidance by the Designated Safeguarding Lead/Student Counsellor.

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 online lessons or engaged in online learning, and report it to the relevant ESLT member of that year group
- Report anything unusual or inappropriate to ESLT and the I.T Team if when accessing your computer, any obscene or inappropriate pop ups, cookies or inadvertent access to inappropriate websites occurs
- Report any inappropriate student behaviors 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

- Report anything unusual or inappropriate 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
- 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 behaviors 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.
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 one Digital Safeguarding Coordinator (DSC) in each phase of the school to monitor, review and develop best practice. The Coordinator will also be the link contact between the Phase and the Designated Digital Safeguarding Officer (DDSO), and Designated Safeguarding Lead (DSL) in all matters of Digital Safeguarding.

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 and DSC, 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 Digital Safeguarding Officer or Coordinators.

School Designated Safeguarding Officer and Digital Safeguarding Coordinators' 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 Officers (DSO's) 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 Acceptable Use Policy and BYOD policy and ensure these are signed by staff, 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 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 Managing Systems

- Monitor that these 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 Acceptable IT Usage Policy.
- 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
- 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 either recorded or/and take place without video.
- 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 DSC's 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.
- 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 an appropriate BYOD and Acceptable Use Policy and understand what the agreements mean,

Parents' Key Responsibilities

- Discuss the school's Acceptable Use Policy and BYOD 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 who 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 school-owned devices that can be used whenever mobile 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.

Monitoring and Review

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

Other documents to refer to are: The Acceptable Use Policy (for children, parents and staff), The EC Professional Code of Conduct (Staff), The BYOD Policy (Students and Parents). These documents/policies are signed each year by the relevant stakeholders.