اكاديمية الدوحة
DOHA ACADEMY

E-Safety Policy

سياسة السلامة الإلكترونية

Contents

1. Purpose:

The purpose of Doha Academy's E-Safety Policy is to establish a comprehensive framework for safeguarding our students while using digital technologies within our school community. This policy outlines our commitment to creating a safe and secure online environment, setting high standards for online behaviour, and ensuring the responsible use of the internet and digital devices in support of teaching and learning.

2. Scope:

This policy applies to all students, staff, and members of our school community who use digital technologies and have access to the internet within the school premises or during school-related activities.

3. Policy Statement:

Our school is committed to ensuring the safety and well-being of our students in the digital age. We recognise the importance of harnessing technology for educational purposes while also protecting students from potential online risks.

4. Teaching and Learning:

4.1 Internet use by students at Doha Academy is intended to enhance student learning. Towards this end, students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.2 Students will be taught to be critically aware of the internet-based materials that they read and shown how to validate information before accepting its accuracy. The school will ensure that the use of materials obtained students complies with academic honesty.

4.3 Students will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. Students are informed that network and Internet use is monitored and inappropriate usage is appropriately followed up.

4.4 Through assemblies, Computer Science, IT and PSHE, students are taught how to behave and how to protect themselves in a digital environment. However, the school does not accept liability for events that occur outside the school.

4.5 Emerging technologies will be examined for educational benefit before use in school is allowed.

4.6 Staff are required to carefully review and adapt materials obtained from the internet to support school work to ensure alignment with Islamic values.

5. Cyberbullying:

5.1 Doha Academy takes the issue and occurrence of cyberbullying seriously. PSHE content about cyberbullying is delivered to students as well as in ICT lessons.

5.2 The school is committed to educating students about the consequences of cyberbullying and the importance of respectful online interactions.

5.3 If the school is aware of any cyberbullying incident within the school, the processes and consequences are the same as those of non-cyberbullying as defined in Doha Academy's Behaviour Management and Anti-Bullying and related policies and procedures.

6. Internet access / Cybersecurity:

6.1 Doha Academy's internet access is designed expressly for student use and includes filtering appropriate to the age of students. The school ensures that the filtering is regularly reviewed and improved. Virus protection is updated regularly and this aspect of internet security is also systematically updated.

6.2 If, even within the filtered digital environment, staff or students discover an unsuitable site, it must be reported to the IT Support team who will take action.

6.3 The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

6.4 Social networking and personal publishing: the school will deny access to social networking sites and students will be advised not to use these at home until they reach the age stipulated by the site administrators.

6.5 Personal Devices: the usage of personal devices by students is outlined in Doha Academy's Bring Your Own Device (BYOD) guidelines. Mobile phones will only be permitted to be used in lessons on teacher instruction. Wearable technology, such as smart watches should be treated in the same way as other devices that allow internet communication.

6.6 While connected to the school network, students are restricted by school filtering and security. Students are required to hand in any smart phone brought to school and that any other device as part of the BYOD initiative does not have a SIM / external internet accessible functionality. If using a mobile network, against the school's guidelines, the school is not accountable for what is accessed by students.

6.7 If a student brings a mobile phone into school and there is evidence that it has been used for taking photographs or filming in school, or there is evidence of inappropriate or indecent images stored on it or there is evidence of cyberbullying, then this will be treated as a serious disciplinary matter and further action will be taken.

7. E-safety concerns and complaints:

7.1 Members of the school's Senior Leadership Team (SLT) will deal with parental or student concerns about e-safety in line with the school's complaint procedure, with matters escalated to the level of the Principal as appropriate.

7.2 Any complaint about staff misuse of the internet must be referred to the Head of School / Principal.

7.3 Complaints of a child protection nature must be immediately dealt with in accordance with Doha Academy's Child Protection Policy and the related procedures.

8. Roles and responsibilities:

The Principal is to:	• be the point of contact for staff misconduct related to internet usage.
Heads of School are to:	• follow through incidences of student misconduct related to internet usage.
Teachers are to:	• deliver content about e-safety and provide reminders when using portable devices in other curriculum areas; • enforce this policy; • deal with matters of cyber bullying, logging such occurrences on the school management information system (ISAMS); • preview any internet content that they intend to share with students.
Designated Safeguarding Leads (DSL):	• follow related Child protection, Safeguarding and Filtering and • Monitoring policies in the case of internet related child abuse.
Students are to:	• follow school guidance and regulations for the use of personal devices and the internet.
Parents are to:	• support the school's e-safety policy and guidelines.
The IT Network Administrator is to:	• accept overarching responsibility for e-safety in the school; • remove access to inappropriate sites as requested by teaching staff; • assume responsibility for the security of the school's system (inclusive of filtering and virus protection) under the direction of the Head of IT Support.

9. Related documents:

- Staff and Student Acceptable Usage Policies
- BYOD Policy
- Behaviour Management policies
- Anti- Bullying Policy
- Child Protection & Safeguarding Policy
- Filtering and Monitoring procedures

Policy Name: Student E-Safety Policy		
Created Date: September 2021	**Last Reviewed Date:** June 2025	**Next reviewed Date:** January 2026
Reviewed By: Principal **Principal Signature:**		**Approved by:** CEO/ Chairperson **CEO/ Chairperson Signature:**
School Stamp:		

اكاديمية الدوحة
DOHA ACADEMY

E-Safety Policy

سياسة السلامة الإلكترونية

1. الغرض:

تهدف سياسة السلامة الإلكترونية في أكاديمية الدوحة إلى إرساء إطار عمل شامل لحماية طلابنا أثناء استخدامهم للتقنيات الرقمية داخل مجتمعنا المدرسي. تُحدد هذه السياسة التزامنا بتهيئة بيئة إلكترونية آمنة، ووضع معايير عالية للسلوك الإلكتروني، وضمان الاستخدام المسؤول للإنترنت والأجهزة الرقمية دعمًا للتعليم والتعلم.

2. النطاق:

تُطبق هذه السياسة على جميع الطلاب والموظفين وأعضاء مجتمعنا المدرسي الذين يستخدمون التقنيات الرقمية ويتصلون بالإنترنت داخل المدرسة أو أثناء الأنشطة المدرسية.

3. بيان السياسة:

تلتزم مدرستنا بضمان سلامة ورفاهية طلابنا في العصر الرقمي. ندرك أهمية تسخير التكنولوجيا لأغراض تعليمية، مع حماية الطلاب من مخاطر الإنترنت المحتملة.

4. التعليم والتعلم:

4.1 يهدف استخدام الطلاب للإنترنت في أكاديمية الدوحة إلى تعزيز تعلمهم. ولتحقيق هذه الغاية، سيتم تثقيف الطلاب حول الاستخدام الفعال للإنترنت في البحث، بما في ذلك مهارات تحديد مصادر المعرفة واسترجاعها وتقييمها.

4.2 سيتم تدريب الطلاب على الوعي النقدي بالمواد الإلكترونية التي يقرؤونها، وكيفية التحقق من صحة المعلومات قبل قبولها. ستضمن المدرسة أن استخدام الطلاب للمواد التي يحصلون عليها يتوافق مع الأمانة الأكاديمية.

4.3 سيتم تعليم الطلاب ما هو مقبول وما هو غير مقبول لاستخدام الإنترنت، وتزويدهم بأهداف واضحة لاستخدامه. سيتم إعلام الطلاب بمراقبة استخدام الشبكة والإنترنت، ومتابعة الاستخدام غير المناسب بشكل مناسب.

4.3 من خلال التجمعات، وعلوم الحاسوب، وتكنولوجيا المعلومات، والتربية الشخصية والاجتماعية والصحية، يتعلم الطلاب كيفية التصرف وحماية أنفسهم في البيئة الرقمية. مع ذلك، لا تتحمل المدرسة مسؤولية أي أحداث تقع خارج المدرسة.

4.5 سيتم فحص التقنيات الناشئة للتحقق من فائدتها التعليمية قبل السماح باستخدامها في المدرسة.

4.6 يُطلب من الموظفين مراجعة المواد التي يتم الحصول عليها من الإنترنت بعناية وتكييفها لدعم العمل المدرسي لضمان توافقها مع القيم الإسلامية.

5 التنمر الإلكتروني:

5.1 تأخذ أكاديمية الدوحة قضية التنمر الإلكتروني ووقوعه على محمل الجد. يُقدّم محتوى تعليمي حول التنمر الإلكتروني للطلاب، بالإضافة إلى دروس تكنولوجيا المعلومات والاتصالات

5.2 تلتزم المدرسة بتثقيف الطلاب حول عواقب التنمر الإلكتروني وأهمية التفاعلات المحترمة عبر الإنترنت.

5.3 في حال علم المدرسة بأي حادثة تنمر إلكتروني داخلها، فإن الإجراءات والعواقب هي نفسها المُطبقة على حالات التنمر غير الإلكتروني، كما هو مُحدد في إدارة السلوك ومكافحة التنمر في أكاديمية الدوحة والسياسات والإجراءات ذات الصلة.

6 الوصول إلى الإنترنت / الأمن السيبراني:

6.1 صُممت خدمة الإنترنت في أكاديمية الدوحة خصيصًا لاستخدام الطلاب، وتتضمن فلترة مناسبة لأعمارهم. وتضمن المدرسة مراجعة الفلترة وتحسينها بانتظام. كما يتم تحديث برامج الحماية من الفيروسات بانتظام، كما يتم تحديث هذا الجانب من أمن الإنترنت بشكل منهجي.

6.2 إذا اكتشف الموظفون أو الطلاب، حتى داخل البيئة الرقمية المُفلترة، موقعًا غير مناسب، فيجب إبلاغ فريق دعم تكنولوجيا المعلومات لاتخاذ الإجراءات اللازمة.

6.3 ستتخذ المدرسة جميع الاحتياطات المعقولة لمنع الوصول إلى المواد غير المناسبة. ومع ذلك، نظرًا للنطاق الدولي وطبيعة محتوى الإنترنت المترابطة، لا يمكن ضمان عدم ظهور المواد غير المناسبة على جهاز كمبيوتر المدرسة. ولا تتحمل المدرسة مسؤولية المواد التي يتم الوصول إليها، أو أي عواقب تترتب على الوصول إلى الإنترنت.

6.4 شبكات التواصل الاجتماعي والنشر الشخصي: ستمنع المدرسة الوصول إلى مواقع التواصل الاجتماعي، ويُنصح الطلاب بعدم استخدامها في المنزل حتى يبلغوا السن التي يحددها مسؤولو الموقع.

6.5 الأجهزة الشخصية: يُحدد استخدام الطلاب للأجهزة الشخصية في إرشادات أكاديمية الدوحة الخاصة بإحضار أجهزتهم الخاصة. يُسمح باستخدام الهواتف المحمولة فقط في الدروس التي تُجرى تحت إشراف المعلم. يجب معاملة الأجهزة القابلة للارتداء، مثل الساعات الذكية، بنفس طريقة معاملة الأجهزة الأخرى التي تتيح الاتصال بالإنترنت.

6.6 أثناء اتصال الطلاب بشبكة المدرسة، يخضعون لقيود أمنية وتصفية. يُطلب من الطلاب تسليم أي هاتف ذكي أحضروه إلى المدرسة، وألا يحتوي أي جهاز آخر ضمن مبادرة إحضار الأجهزة الشخصية على شريحة SIM خاصية الوصول إلى الإنترنت الخارجي. في حال استخدام شبكة جوال، بما يخالف إرشادات المدرسة، فإن المدرسة غير مسؤولة عما يصل إليه الطلاب.

6.7 إذا أحضر طالب هاتفًا محمولًا إلى المدرسة، وثبت استخدامه لالتقاط الصور أو مقاطع الفيديو داخل المدرسة، أو وجود صور غير لائقة أو مخبأة عليه، أو وجود دليل على التنمر الإلكتروني، فسيتم التعامل مع ذلك كمسألة تأديبية خطيرة، وسيتم اتخاذ إجراءات إضافية.

7 مخاوف وشكاوى السلامة الإلكترونية:

7.1 سيتعامل أعضاء فريق القيادة العليا بالمدرسة مع مخاوف أولياء الأمور أو الطلاب بشأن السلامة الإلكترونية وفقًا لإجراءات الشكاوى المتبعة في المدرسة، مع تصعيد الأمور إلى مستوى مدير المدرسة حسب الاقتضاء.

7.2 يجب إحالة أي شكوى تتعلق بإساءة استخدام الموظفين للإنترنت إلى رئيس المدرسة/مدير المدرسة.

7.3 يجب التعامل مع الشكاوى المتعلقة بحماية الطفل فورًا وفقًا لسياسة حماية الطفل في أكاديمية الدوحة والإجراءات ذات الصلة.

8 الأدوار والمسؤوليات:

على مدير المدرسة:	أن يكون جهة الاتصال في حال حدوث أي سوء سلوك من قبل الموظفين فيما يتعلق باستخدام الإنترنت.
على رؤساء المدارس:	متابعة حالات سوء سلوك الطلاب فيما يتعلق باستخدام الإنترنت.
على المعلمين:	• تقديم محتوى حول السلامة الإلكترونية وتذكير الطلاب عند استخدام الأجهزة المحمولة في مجالات دراسية أخرى؛ • تطبيق هذه السياسة؛ • التعامل مع قضايا التنمر الإلكتروني، وتسجيل مثل هذه الحوادث على نظام معلومات إدارة المدرسة (ISAMS)؛ • معاينة أي محتوى على الإنترنت يعتزمون مشاركته مع الطلاب.
على مسؤولي السلامة المعينين:	مسؤولي الحماية المعينين: • اتباع سياسات حماية الطفل والحماية والتصفية ذات الصلة • ومراقبة حالات إساءة معاملة الأطفال عبر الإنترنت.
على الطلاب:	اتباع إرشادات المدرسة ولوائحها المتعلقة باستخدام الأجهزة الشخصية والإنترنت.
على أولياء الأمور:	دعم سياسة وإرشادات السلامة الإلكترونية في المدرسة.
على مسؤول شبكة تكنولوجيا المعلومات:	• تحمل المسؤولية الشاملة عن السلامة الإلكترونية في المدرسة؛ • إزالة إمكانية الوصول إلى المواقع غير المناسبة بناءً على طلب هيئة التدريس؛ • تحمل مسؤولية أمن نظام المدرسة (بما في ذلك الفلترة والحماية من الفيروسات) تحت إشراف رئيس دعم تكنولوجيا المعلومات.

9 الوثائق ذات الصلة:

- سياسات الاستخدام المقبول للموظفين والطلاب
- سياسة إحضار جهازك الخاص
- سياسات إدارة السلوك
- سياسة مكافحة التنمر
- سياسة حماية الطفل وسلامته
- إجراءات التصفية والمراقبة

اسم السياسة: سياسة السلامة الإلكترونية		
تاريخ الإنشاء: سبتمبر 2021	تاريخ آخر مراجعة: يونيو 2025	تاريخ المراجعة التالية: يناير 2026
مُعتمد من المدير: التوقيع:		مُعتمد من الرئيس التنفيذي: التوقيع:
ختم المدرسة:		ختم المجموعة:

أكاديمية الدوحة ذ.م.م
ص.ب: ٩٦٩١، الدوحة - قطر
P.O.Box: 9691, Doha-Qatar
Doha Academy W.L.L