مدرسة جيمس كامبريدج العالمية أبوظبي
GEMS Cambridge International School
ABU DHABI

سياسة إحضار الأجهزة الشخصية (BYOD)

معلومات السياسة

البند	التفاصيل
عنوان السياسة	سياسة إحضار الأجهزة الشخصية (BYOD)
المدرسة	مدرسة جيمس كامبريدج العالمية – أبوظبي
نوع السياسة	سياسة خاصة بالطلبة
الجهة المعتمِدة	مدير المدرسة / الرئيس التنفيذي
تاريخ السريان	العام الدراسي 2026-2027
دورة المراجعة	مراجعة سنوية
تاريخ المراجعة الرسمية	أغسطس 2028 أو في موعد أقرب عند الاقتضاء
الجهة المسؤولة عن السياسة	مدير المدرسة / الرئيس التنفيذي

1 – الغرض

تُدرك مدرسة جيمس كامبريدج العالمية – أبوظبي («المدرسة») أن التكنولوجيا يمكن أن تعزّز التعلّم والإبداع والتواصل وإمكانية الوصول ومشاركة الطلبة متى استُخدمت بمسؤولية وأمان.

تضع هذه السياسة التوقعات والمسؤوليات والضمانات التي تحكم استخدام الطلبة للأجهزة الرقمية المملوكة لهم شخصيًا.

تهدف هذه السياسة إلى: دعم التعليم والتعلّم، وتعزيز السلوك الرقمي الآمن والمسؤول، وحماية رفاهية الطلبة وخصوصيتهم، وصون أنظمة المدرسة ومعلوماتها، وتعزيز الأمن السيبراني وحماية البيانات، ودعم النزاهة الأكاديمية، ووضع إجراءات واضحة للإبلاغ عن المخاوف والحوادث؛ وضمان الامتثال للمتطلبات المعمول بها لدى «جيمس» ودائرة التعليم والمعرفة ودولة الإمارات العربية المتحدة. إن الوصول إلى شبكات المدرسة وأنظمتها وخدماتها الرقمية امتياز وليس حقًا مكتسبًا، ويرتبط بالتزام الطالب بهذه السياسة.

2 – النطاق

تسري هذه السياسة على جميع طلبة المدرسة الذين يستخدمون أجهزة مملوكة لهم شخصيًا أو أجهزة مصرّحًا بها من المدرسة، وذلك: داخل مرافق المدرسة، وخلال اليوم الدراسي، وفي وسائل النقل المدرسي حيثما تنطبق قواعد المدرسة، وخلال الزيارات التعليمية والرحلات والمسابقات والأنشطة اللاصفية، وأثناء التعلّم عبر الإنترنت أو عن بُعد، وعند الدخول إلى حسابات المدرسة أو منصاتها أو أنظمتها؛ وفي أي وقت تُستخدم فيه التكنولوجيا لأغراض تتعلق بالمدرسة.

تسري السياسة على: أجهزة الحاسوب المحمولة، والأجهزة اللوحية، والهواتف المحمولة، والساعات الذكية، والأجهزة المزوّدة بشريحة اتصال (SIM)، والأجهزة المتصلة بالإنترنت، والأجهزة الطرفية والملحقات الرقمية؛ والتقنيات المستقبلية القادرة على إنشاء المعلومات أو تخزينها أو معالجتها أو تسجيلها أو مشاركتها.

في حال توفير أجهزة صادرة عن المدرسة أو معارة من قِبلها للطلبة، تنطبق متطلبات الحماية والسلوك والاستخدام المقبول والسلامة الرقمية الواردة في هذه السياسة بالقدر نفسه، ما لم يوجد إجراء مدرسي أكثر تحديدًا.

يخضع استخدام الموظفين والزوار للأجهزة لسياسات منفصلة صادرة عن «جيمس» والمدرسة.

3 – المبادئ العامة

يجب أن يكون استخدام الطلبة للتكنولوجيا دائمًا: داعمًا للتعلّم، ومناسبًا للعمر، وحاميًا لسلامة جميع المستخدمين ورفاهيتهم، ومحترمًا لحقوق الآخرين وكرامتهم وخصوصيتهم، وممتثلًا لمتطلبات حماية الطلبة في المدرسة، وداعمًا للأمانة الأكاديمية، وحاميًا لمعلومات المدرسة وأنظمتها، وممتثلًا لقوانين دولة الإمارات العربية المتحدة وأعرافها الثقافية؛ ومتّبعًا لتعليمات الموظفين.

يجوز أن يُطلب من الطالب في أي وقت: التوقف عن استخدام الجهاز، أو إغلاق التطبيقات، أو تأمين الجهاز، أو إيقاف تشغيله؛ أو تسليمه مؤقتًا وفقًا لإجراءات المدرسة.

4 – الأجهزة المعتمدة والمتطلبات التقنية

تحدد المدرسة فئات الأجهزة التي يجوز استخدامها في كل مرحلة دراسية أو مجموعة صفية.

يجوز للمدرسة نشر متطلبات تقنية منفصلة توضح: أنواع الأجهزة المعتمدة، والحد الأدنى لأنظمة التشغيل، ومتطلبات المتصفحات، ومتطلبات التحديثات الأمنية، ومتطلبات برامج مكافحة الفيروسات عند الاقتضاء، ومتطلبات توافق الشبكة، والتوقعات المتعلقة بالبطارية، ومتطلبات التخزين، والتوقعات المتعلقة بالشحن؛ ومتطلبات الأغلفة الواقية.

يتحمل الطلبة وأولياء الأمور مسؤولية التأكد من أن الأجهزة: بحالة تشغيل جيدة، ومحدّثة، وتستخدم كلمة مرور أو رمزًا سريًا آمنًا، ومزوّدة بحماية أمنية مناسبة، وتصل إلى المدرسة بشحن كافٍ، وتستوفي متطلبات المدرسة؛ ولا تحتوي على برمجيات يُقصد بها مهاجمة الأنظمة أو الشبكات أو تجاوزها أو التدخل فيها. وقد يؤدي عدم استيفاء المتطلبات التقنية إلى فقدان إمكانية الوصول إلى الشبكة.

5 – الاستخدام المسموح به

يجوز للطلبة استخدام جهاز مصرّح به عندما يوجّههم المعلم أو يوافق على ذلك، للأغراض التالية على سبيل المثال: البحث، والأعمال الصفية، والأعمال الدراسية المقررة، والواجبات المنزلية، وأعمال المشاريع، والتعاون الرقمي، والبرامج التعليمية المعتمدة، والكتب الدراسية الرقمية، والتقنيات المساندة، والتقييمات المعتمدة؛ والتعلّم المدعوم بالذكاء الاصطناعي المعتمد.

خلال الحصص الدراسية، يجب على الطلبة: اتباع تعليمات المعلم، واستخدام المصادر المعتمدة فقط، والبقاء منشغلين بالمهمة، وإبقاء الأجهزة متاحة للإشراف، والتوقف عن الاستخدام فورًا عند الطلب؛ وتجنّب تشتيت أنفسهم أو الآخرين.

6 – الاستخدام المحظور

يُحظر على الطلبة: تعطيل التعليم والتعلّم، والوصول إلى محتوى غير لائق، وممارسة التنمر الإلكتروني، ومضايقة الآخرين أو تهديدهم أو ترهيبهم، وانتحال شخصية أي فرد، والدخول إلى حساب شخص آخر، ومشاركة كلمات المرور، ومحاولة الوصول غير المصرّح به إلى الأنظمة أو المعلومات، وتثبيت برمجيات غير مصرّح بها، وإجراء أنشطة فحص الشبكات أو الاختراق، والمقامرة، وبث محتوى غير تعليمي، واستخدام وسائل التواصل الاجتماعي لأغراض غير تعليمية، ونشر المعلومات المضللة، وإساءة استخدام الذكاء الاصطناعي، والغش أو الانتحال، وإفشاء المعلومات السرية، ونقل معلومات المدرسة إلى خدمات شخصية؛ أو استخدام التكنولوجيا بطرق تخالف توقعات المدرسة أو القانون المعمول به.

7 – الشبكات الافتراضية الخاصة (VPN) وأدوات تجاوز الحماية

يجب على الطلبة استخدام شبكات المدرسة المعتمدة فقط.

يُحظر على الطلبة استخدام: الشبكات الافتراضية الخاصة (VPN)، وخدمات الوكيل (Proxy)، وخدمات إخفاء الهوية، ونقاط الاتصال الشخصية (Hotspot)، ومشاركة اتصال الإنترنت (Tethering)، وخدمات أنظمة أسماء النطاقات (DNS) البديلة؛ أو أي تقنية يُقصد بها تجاوز الحجب أو المراقبة المطبقة في المدرسة. ويُحظر استخدام بيانات الهاتف المحمول لتجنّب ضوابط الحماية المعمول بها في المدرسة.

8 – الهواتف المحمولة والساعات الذكية والأجهزة المزوّدة بشريحة اتصال (SIM)

لا يُسمح للطلبة باستخدام الهواتف المحمولة الشخصية خلال اليوم الدراسي.

يجوز الموافقة على استثناءات: لنشاط تعليمي محدد، أو لحاجة طبية موثقة، أو لحاجة تتعلق بإمكانية الوصول؛ أو لمتطلب يتعلق بالحماية. وفي حال عدم وجود استثناء، يجب إبقاء الأجهزة مؤمَّنة وغير مستخدمة. ويجب تعطيل وظائف الاتصال في الساعات الذكية والأجهزة المزوّدة بشريحة اتصال أثناء التواجد في المدرسة، ما لم ينطبق استثناء رسمي. ولا تُعدّ الهواتف المحمولة والساعات الذكية أجهزة تعلّم معتمدة ضمن برنامج المدرسة لإحضار الأجهزة الشخصية (BYOD).

9 – التصوير والتسجيل الصوتي والمرئي

يُحظر على الطلبة التصوير الفوتوغرافي أو تصوير الفيديو أو التسجيل الصوتي أو تسجيل الشاشة أو البث المباشر أو نشر محتوى يتعلق بـ: الطلبة، أو الموظفين، أو الزوار، أو مستندات المدرسة، أو أنظمتها، أو المعلومات السرية؛ أو أنشطة المدرسة، دون إذن صريح.

يُحظر على الطلبة إنشاء أو توزيع: تسجيلات مؤذية، أو محتوى مهين، أو وسائط معدّلة، أو محتوى مزيّف بتقنية التزييف العميق، أو تسجيلات لحوادث سلوكية، أو مواد امتحانات، أو محتوى متعلق بحماية الطلبة؛ أو معلومات سرية.

10 – وسائل التواصل الاجتماعي

لا يجوز للطلبة الدخول إلى وسائل التواصل الاجتماعي: خلال اليوم الدراسي، أو عبر أنظمة المدرسة، أو عبر شبكاتها؛ أو خلال الأنشطة التي تشرف عليها المدرسة، ما لم يُصرَّح بذلك صراحةً لأغراض تعليمية.

يُحظر على الطلبة: إنشاء حسابات تمثّل المدرسة، أو عرض آراء شخصية على أنها تواصل رسمي صادر عن المدرسة، أو نشر معلومات سرية، أو رفع صور أو تسجيلات غير مصرّح بها؛ أو الانخراط في سلوك إلكتروني ضار أو تهديدي أو تمييزي.

11 – مسؤوليات حماية الطلبة

يجب على الطلبة: استخدام الأجهزة بأمان ومسؤولية، وحماية المعلومات الشخصية، والحفاظ على سرية كلمات المرور، والتواصل باحترام، واستخدام المنصات المعتمدة، والإبلاغ الفوري عن أي مخاوف؛ واتباع توجيهات الموظفين.

يجب على الطلبة الإبلاغ فورًا عن: المحتوى الضار، والتنمر الإلكتروني، والمراسلات المشبوهة، وعمليات الاحتيال، ومحاولات التصيّد الاحتيالي، واختراق الحسابات، والطلبات غير اللائقة، والمخاوف المتعلقة بالحماية؛ أو أي أمر عبر الإنترنت يثير القلق أو الضيق. ولن يتعرّض الطلبة لأي ضرر نتيجة تقديمهم بلاغات حماية صادقة.

12 – الذكاء الاصطناعي وأدوات التعلّم الرقمي

يجوز للطلبة استخدام أدوات الذكاء الاصطناعي فقط عندما: تصرّح بها المدرسة، وتُعتمد وفق إجراءات المدرسة و«جيمس» المعمول بها، ويوافق عليها المعلم، وتُستخدم لغرض تعلّمي محدد، وتتوافر الضمانات المناسبة؛ ويلتزم الطلبة بتعليمات المعلم. ولا يجوز للطلبة استخدام سوى أدوات الذكاء الاصطناعي المصرّح بها تحديدًا من المدرسة لأنشطة التعلّم. ولا تُعدّ اشتراكات الذكاء الاصطناعي الشخصية، والحسابات التي ينشئها الطلبة بأنفسهم، وأدوات الذكاء الاصطناعي الاستهلاكية المتاحة للعامة معتمدةً تلقائيًا للاستخدام المدرسي.

يُحظر على الطلبة استخدام الذكاء الاصطناعي في: الغش، أو الانتحال، أو تلفيق المعلومات، أو انتحال شخصية الآخرين، أو تجاوز متطلبات التقييم، أو إنتاج محتوى ضار، أو إنشاء محتوى مزيّف بتقنية التزييف العميق، أو نشر المعلومات المضللة، أو انتهاك حقوق النشر؛ أو تحريف نسبة العمل إلى صاحبه. ويجب أن يكمّل الذكاء الاصطناعي التعلّم لا أن يحلّ محل تفكير الطالب وإبداعه وجهده.

13 – موافقة استخدام الذكاء الاصطناعي والبيانات الشخصية

إن الموافقة على هذه السياسة لا تُعدّ موافقةً على قيام منصة محددة للذكاء الاصطناعي بمعالجة بيانات الطلبة.

وحيثما تكون هناك حاجة إلى موافقة منفصلة، ستحصل المدرسة على موافقة ولي الأمر عبر إجراء معتمد.

يُحظر على الطلبة رفع أو إدخال معلومات شخصية أو مدرسية أو عائلية في أدوات الذكاء الاصطناعي أو الخدمات الرقمية غير المعتمدة.

14 – النزاهة الأكاديمية وحقوق النشر

يجب على الطلبة: إنتاج أعمال أصيلة، والإشارة إلى المصادر بالشكل المناسب، والالتزام بقواعد التقييم، واتباع تعليمات المعلم، واحترام حقوق النشر، واحترام الملكية الفكرية؛ والإفصاح بدقة عن استخدام الذكاء الاصطناعي حيثما يُطلب ذلك. ولا يُعفي استخدام الأدوات الرقمية الطالب من مسؤوليته عن دقة العمل المقدَّم وأصالته.

15 – حماية البيانات والخصوصية

يجب على الطلبة: حماية المعلومات الشخصية، وحماية معلومات المدرسة، وتجنّب مشاركة المعلومات السرية، واستخدام الأنظمة المعتمدة فقط؛ والإبلاغ الفوري عن أي مخاوف.

يجب على الطلبة الإبلاغ فورًا عن: الأجهزة المفقودة، والأجهزة المسروقة، والحسابات المخترَقة، وانتهاكات الخصوصية، والإفصاح العرضي عن المعلومات، والاشتباه في تسرّب البيانات، وحوادث التصيّد الاحتيالي؛ والوصول غير المصرّح به. ويجب على الطلبة الإبلاغ فورًا عن أي جهاز شخصي مفقود أو مسروق أو غير معلوم المكان أُحضر إلى مرافق المدرسة، سواء أكانت معلومات المدرسة مخزنة على ذلك الجهاز أم لا.

16 – إمكانية الوصول واحتياجات التعلّم الإضافية

ستوفّر المدرسة التسهيلات المعقولة عند الحاجة.

يجوز اعتماد التقنيات المساندة وترتيبات إمكانية الوصول من خلال: خطط التعلّم الموثقة، أو الخطط الطبية، أو ترتيبات الحماية؛ أو الإجراءات المدرسية المعتمدة. ولن يتضرر أي طالب أكاديميًا لأن أسرته لا تملك جهازًا رقميًا مناسبًا. وحيثما يلزم جهاز شخصي، ستنظر المدرسة في ترتيبات بديلة معقولة وفقًا للإمكانات المتاحة.family does not own a suitable digital device. Where a personal device is required, the school will consider reasonable alternative arrangements subject to available provision.

---

17 – الرفاهية الرقمية

تشجّع المدرسة على استخدام التكنولوجيا بشكل صحي ومتوازن ومناسب للعمر.

ينبغي أن تدعم التكنولوجيا: التعلّم، والإبداع، والرفاهية، والعلاقات؛ والتطور الشخصي.

يجوز للمدرسة تقديم إرشادات بشأن: الاستخدام الصحي للشاشات، والنوم والتكنولوجيا، والمرونة الرقمية، والسلوك الآمن عبر الإنترنت، واستخدام وسائل التواصل الاجتماعي، والألعاب الإلكترونية المسؤولة، وإدارة التشتت الرقمي؛ وتحقيق التوازن بين الأنشطة عبر الإنترنت وخارجها. وفي حال وجود مخاوف بشأن الاستخدام المفرط أو الضار للتكنولوجيا، يجوز للمدرسة اتخاذ تدخلات مناسبة تتعلق بالرفاهية أو السلوك أو الحماية أو الرعاية الطلابية.

---

18 – المراقبة والخصوصية

تطبّق المدرسة ضوابط الحجب والمراقبة والوصول على أنظمة المدرسة وشبكاتها.

يجوز للمدرسة مراقبة النشاط الذي يتم عبر: حسابات المدرسة، وأنظمتها، وشبكاتها؛ ومنصات التعلّم المعتمدة.

قد تُجرى المراقبة لأغراض: حماية الطلبة، والأمن السيبراني، والامتثال، والتحقيق، والرفاهية، والأمن التشغيلي؛ وحماية المجتمع المدرسي. ولا تراقب المدرسة بصورة اعتيادية المحتوى الشخصي غير المتعلق بنشاط المدرسة والمخزّن على الأجهزة الخاصة.

---

19 – الحوادث الرقمية

تشمل الحوادث الرقمية: التنمر الإلكتروني، وإساءة استخدام الذكاء الاصطناعي، وانتهاكات الخصوصية، والمحتوى غير اللائق، والتصيّد الاحتيالي، والبرمجيات الخبيثة، وفقدان البيانات، واختراق الحسابات، والوصول غير المصرّح به، والمراسلات الضارة؛ ومحاولات تجاوز ضوابط المدرسة. ويجب الإبلاغ عن الحوادث فورًا.

ستقوم المدرسة بما يلي: التحقيق، وحفظ الأدلة، ودعم الطلبة المتضررين، وإشعار أولياء الأمور عند الاقتضاء، واتباع إجراءات الحماية، واتباع إجراءات الأمن السيبراني، والاحتفاظ بالسجلات؛ وإحالة الأمور إلى الجهات الخارجية عند الاقتضاء. وسيُسجَّل كل حادث رقمي رسمي ويراجعه مدير المدرسة / الرئيس التنفيذي ويُحتفظ به وفقًا لمتطلبات حفظ السجلات المعمول بها.

---

20 – عواقب إساءة الاستخدام

قد تؤدي إساءة الاستخدام إلى: الإنذارات، وإجراءات تصالحية، وسحب امتيازات استخدام الجهاز، وإيقاف الوصول إلى الشبكة، والمصادرة المؤقتة، والتواصل مع ولي الأمر، وتدخلات سلوكية، وتدخلات متعلقة بالحماية، وإجراءات تأديبية، والإحالة إلى إجراءات «جيمس»؛ أو الإحالة إلى الجهات المختصة عند الاقتضاء.

---

21 – مسؤوليات أولياء الأمور والأوصياء

يُتوقع من أولياء الأمور: دعم هذه السياسة، ومناقشة التوقعات مع أبنائهم، ومتابعة الاستخدام المناسب للأجهزة خارج المدرسة، واستخدام أدوات الرقابة الأبوية حيثما تتوافر، ومتابعة استخدام وسائل التواصل الاجتماعي، والتأكد من استيفاء الأجهزة للمتطلبات، والتعاون مع التحقيقات؛ والإبلاغ عن أي مخاوف دون تأخير. وينبغي لأولياء الأمور توفير ترتيبات تأمين وحماية مناسبة لأجهزة الطلبة.

---

22 – الفقدان والتلف والمسؤولية

تُحضَر الأجهزة الشخصية إلى المدرسة على مسؤولية مالكها.

لا توفر المدرسة تأمينًا للأجهزة الشخصية ولا تتحمل المسؤولية عن: الصيانة، أو الإصلاح، أو الترقيات، أو الملحقات، أو توفير الشحن؛ أو النسخ الاحتياطي للبيانات الشخصية. وتُشجَّع الأسر على التأمين على الأجهزة بالشكل المناسب.

---

23 – التواصل والنشر والإرشادات المناسبة للعمر

ستُنشر هذه السياسة عبر قنوات المدرسة، وتُتاح لأولياء الأمور، ويُشار إليها في الإرشادات المدرسية، وتُدعم من خلال التربية على المواطنة الرقمية؛ وتُراجع سنويًا.

ستوفّر المدرسة إرشادات مناسبة للعمر لكل من: من FS1 إلى Year 2، ومن Year 3 إلى Year 7؛ ومن Year 8 إلى Year 13. وستُراجع وثائق الإرشاد هذه سنويًا لضمان استمرار توافقها مع المتطلبات التنظيمية والاحتياجات التنموية للطلبة. وسيُتاح لأولياء الأمور الاطلاع على السياسة كاملةً.

---

24 – التدريب

سيتلقى الطلبة إرشادات حول: السلامة الرقمية، والأمن السيبراني، والخصوصية، وحماية الطلبة، والاستخدام المسؤول للذكاء الاصطناعي، والنزاهة الأكاديمية، والتهديدات السيبرانية، والتواصل عبر الإنترنت؛ والإبلاغ عن المخاوف. وسيُقدَّم التدريب المناسب قبل أن يستخدم الطلبة أدوات التعلّم القائمة على الذكاء الاصطناعي والمعتمدة من المدرسة.

---

25 – الحوكمة والمراجعة

يتولى مدير المدرسة / الرئيس التنفيذي المسؤولية الشاملة عن التنفيذ.

ستُراقَب السياسة من خلال: سجلات الحماية، وسجلات السلوك، وسجلات الحوادث، ومعلومات الرفاهية الرقمية، ومعلومات الأمن السيبراني، ونتائج التدقيق، وملاحظات أولياء الأمور، وملاحظات الطلبة؛ والمستجدات التنظيمية. وستُراجَع السياسة سنويًا وتُجدَّد رسميًا في موعد أقصاه أغسطس 2028.