



الدار للتعليم - شركة الشخص الواحد ذ.م.م

دليل سياسة الاستخدام المسؤول لأنظمة معلومات الدار للتعليم

معلومات الوثيقة

الاسم	دليل سياسة الاستخدام المسؤول لأنظمة معلومات الدار للتعليم
الرقم المرجعي	ALDED-EDT-GEN-PL-00001

مراقبة إصدار الوثيقة

الإصدار	التاريخ	ملخص التغيير
الإصدار 1	2 سبتمبر 2025	الإصدار الأولي

التصنيف: للاستخدام الداخلي

- أ- مقدمة..... 3
- 1- العنوان:..... 3
- 2- الغرض..... 3
- 3- الوثيقة الحاكمة..... 3
- 4- النطاق..... 3
- 5- الامتثال..... 4
- ب- بيانات السياسة..... 4
- 1- الأدوار والمسؤوليات..... 4
- 2- استخدام أنظمة/موارد معلومات الدار للتعليم..... 4
- 3- استخدام النسخ غير المصرح بها من البرمجيات والأجهزة المرخصة..... 5
- 4- استخدام التطبيقات المجانية والمشاركة..... 5
- 5- استخدام المواد المحمية بحقوق الطبع والنشر والأدوات الرقمية..... 6
- 6- إدخال المواد الإباحية..... 6
- 7- إدخال البرامج التخريبية..... 7
- 8- الخصوصية والسرية..... 7
- 9- العمل خارج الموقع..... 7
- 10- الإجراءات عند إنهاء العقد أو ترك المدرسة..... 7
- 11- استخدام الإنترنت..... 7
- 12- حماية المعلومات..... 9
- 13- الإقرارات العامة..... 9
- 14- البريد الإلكتروني (EMAIL)..... 9
- 15- مكافحة الفيروسات..... 11
- 16- تخزين البيانات على ONEDRIVE / SHAREPOINT..... 12
- 17- المراسلة الفورية (IM)..... 12
- 18- العناية الواجبة..... 13
- ج- التعريفات..... 13

أ- مَقْدَمَة

1- العنوان:

1-1 تُعرف هذه الوثيقة بـ "دليل سياسة الاستخدام المسؤول لأنظمة معلومات الدار للتعليم" ("السياسة").

2- الغرض

1-2 صيغت هذه السياسة لإرساء الضوابط التالية:

1-1-2 ضمان الاستخدام الملائم لأنظمة ومرافق معلومات الدار للتعليم في تسيير الأعمال.

2-1-2 تهيئة بيئة تُعزز الممارسات الأمنية السليمة والاستخدام الفعال لموارد العمل.

3-1-2 ضمان وصول الشركة إلى موارد تقنية موثوقة وقوية ومحمية من الاستخدام غير المصرح به أو الخبيث.

3- الوثيقة الحاكمة

1-3 يجب قراءة دليل السياسة هذا بالاقتران مع ما يلي:

1-1-3 المرسوم بقانون اتحادي رقم (38) لسنة 2021 بشأن حقوق المؤلف والحقوق المجاورة، و

2-1-3 آيزو 27001:2022.

4- النطاق

1-4 ما لم يُنص على خلاف ذلك، تُلزم هذه السياسة وتُطبق على:

1-1-4 جميع الموظفين العاملين في المقر الرئيسي للدار للتعليم، وأكاديمية الدار للتدريب، ومدارسها المُشغَّلة، والطلاب، والمقاولين،

وأي أفراد أو كيانات أخرى قد تستخدم موارد المعلومات وتقنية المعلومات التابعة للدار للتعليم (يشار إليهم فيما بعد بلفظ

"المستخدم"). بالنسبة للمدارس المُدارة، يُرجع إلى هذه السياسة في المجالات التي تقع ضمن مسؤولية الدار للتعليم وفقاً

للاتفاقية القانونية ذات الصلة.

2-1-4 أنظمة المعلومات التي تملكها أو تستأجرها الدار للتعليم (يشار إليها فيما بعد بلفظ "الدار للتعليم") وأي أجهزة خاصة متصلة

بشبكة الدار للتعليم، وتشمل على سبيل المثال لا الحصر أجهزة الكمبيوتر، والأجهزة اللوحية، والبرمجيات، وأنظمة التشغيل،

ووسائط التخزين، والإنترنت.

2-4 ليس في هذه السياسة ما يبطل أي إجراءات سابقة اتُخذت بصورة صحيحة بموجب وثائق سابقة.

3-4 تعالج هذه السياسة المجالات التالية:

1-3-4 الأدوار والمسؤوليات،

2-3-4 استخدام أنظمة/موارد معلومات الدار للتعليم،

3-3-4 استخدام النسخ غير المصرح بها من البرمجيات والأجهزة المرخصة،

4-3-4 استخدام التطبيقات المجانية والمشاركة،

5-3-4 استخدام المواد المحمية بحقوق الطبع والنشر والأدوات الرقمية،

6-3-4 إدخال المواد الإباحية،

7-3-4 إدخال البرامج التخريبية،

8-3-4 الخصوصية والسرية،

9-3-4 العمل خارج الموقع،

10-3-4 الإجراءات عند إنهاء العقد أو ترك المدرسة،

11-3-4 استخدام الإنترنت،

12-3-4 حماية المعلومات،

13-3-4 الإقرارات العامة،

14-3-4 البريد الإلكتروني،

15-3-4 مكافحة الفيروسات،

16-3-4 تخزين البيانات على OneDrive / SharePoint،

17-3-4 المراسلة الفورية (IM)،

18-3-4 العناية الواجبة، و

5- الامتثال

1-5 قد تؤدي مخالفة هذه السياسة والوثائق الداعمة لها إلى إجراءات تصحيحية من قبل السلطات الإدارية المعنية. ويجرى التحقيق التأديبي بما يتناسب مع خطورة الحادثة، حسبما يحدده التحقيق.

2-5 يجب الإبلاغ فوراً عن أي حالة عدم امتثال أو خرق لهذه السياسة إلى مكتب خدمة الدار للتعليم على sd@aldareducation.com لاتخاذ الإجراءات الفورية وحل المشكلة.

3-5 توجه جميع الاستفسارات المتعلقة بتفسير دليل السياسة هذا إلى مكتب خدمة الدار للتعليم على sd@aldareducation.com.

4-5 يجب استخدام النسخة المعتمدة فقط من هذه السياسة، والنسخ المطبوعة غير الخاضعة للرقابة لن تُعتبر سارية.

ب- بيانات السياسة

1- الأدوار والمسؤوليات

1-1 يتعين على كل مستخدم لموارد الخدمات الرقمية والتقنية التابعة للدار للتعليم الإلمام بالسياسات ذات الصلة وممارسة أنشطته ضمن نطاق هذه السياسات.

2- استخدام أنظمة/موارد معلومات الدار للتعليم

1-2 يعد أي استكشاف أو بحث في النطاق العام يتعلق بالعمل مقبولاً شريطة امتثال المستخدمين لسياسة ومعايير وإجراءات الدار للتعليم المتعلقة بهذا الاستخدام، مع الامتثال أيضاً لسياسات ومعايير وإجراءات الموقع الذي يجري استكشافه.

2-2 يجب أن يتوافق استخدام أنظمة المعلومات ومواردها مع سياسات الموارد البشرية والثقافة في الشركة وسياسة مدونة قواعد السلوك التجاري لمجموعة الدار.

3-2 يُحظر على المستخدمين النهائيين ما يلي:

1-3-2 استخدام أنظمة معلومات الدار للتعليم لأغراض لا تتعلق بأنشطة الشركة/المدرسة.

2-3-2 استخدام الموارد لأسباب شخصية أو نيابة عن الغير (مثل عميل شخصي، فرد من العائلة، منظمات سياسية/دينية/خيرية أو مدرسية، وما إلى ذلك).

3-3-2 استخدام معرف مستخدم وكلمة مرور شخص آخر للوصول إلى أنظمة الخدمات الرقمية والتقنية التابعة للدار للتعليم.

4-3-2 ترك حسابات المستخدمين الخاصة بهم مسجلة الدخول على جهاز كمبيوتر غير مراقب وغير مؤمن.

5-3-2 ترك كلمات المرور الخاصة بهم دون حماية (على سبيل المثال، تدوينها).

6-3-2 إجراء أي تغييرات غير مصرح بها على أنظمة أو معلومات الخدمات الرقمية والتقنية التابعة للدار للتعليم.

7-3-2 محاولة الوصول إلى بيانات غير مصرح لهم باستخدامها أو الوصول إليها.

8-3-2 تجاوز حدود صلاحياتهم أو احتياجات العمل المحددة للوصول إلى النظام أو البيانات.

- 9-3-2 توصيل أي جهاز غير مصرح به من الدار للتعليم بالشبكة الداخلية أو بنظام الخدمات الرقمية والتقنية التابع لها.
- 10-3-2 نقل بيانات الدار للتعليم على أي جهاز غير مصرح به.
- 11-3-2 استخدام أنظمة معلومات الدار للتعليم لتخزين أو معالجة أو تنزيل أو نقل بيانات يمكن تفسيرها على أنها متحيزة (سياسيًا، دينيًا، عرقيًا، إثنيًا، وما إلى ذلك) أو داعمة للتحرش.
- 12-3-2 تنزيل أو إعادة توزيع أو طباعة مقالات أو مستندات أو مواد أخرى محمية بحقوق الطبع والنشر عبر أنظمة معلومات الدار للتعليم.
- 13-3-2 استلام أو طباعة أو نقل أو نشر بيانات مملوكة أو أسرار الشركة أو معلومات سرية أخرى بما يخالف سياسة الشركة أو الاتفاقيات الخاصة بالملكية.
- 14-3-2 تنزيل مواد غير لائقة مثل ملفات الصور أو ملفات الموسيقى أو ملفات الفيديو للاستخدام الشخصي.
- 15-3-2 الدخول في تفاعلات غير آمنة عبر الإنترنت، بما في ذلك التواصل مع مستخدمين ينتحلون هويات مزيفة أو مضللة.
- 16-3-2 إظهار سلوك شخصي عبر الإنترنت قد يسبب ضررًا للنفس أو للآخرين، مثل المشاركة في التمر الإلكتروني أو التشجيع عليه.
- 17-3-2 المشاركة في أو التعرض لمخاطر مالية عبر أنظمة الدار للتعليم، بما في ذلك عمليات الاحتيال عبر الإنترنت أو المقامرة أو أنشطة التصيد الاحتيالي.
- 4-2 يتعين على الطلاب في مدارس الدار للتعليم الالتزام باستخدام أجهزةهم الشخصية عبر شبكة الدار للتعليم بما يتوافق مع سياسة "أحضر جهازك الخاص" المعتمدة من قبل المؤسسة. ينطبق ذلك على جميع مرافق المدرسة وكذلك أثناء المشاركة في الأنشطة اللاصفية التي تقام خارج المباني المدرسية.
- 5-2 يجب على الطلاب شراء "باقة السلامة الرقمية" لتسجيل أجهزةهم في نظام إدارة الأجهزة المحمولة (MDM) الخاص بالدار للتعليم.
- 6-2 يجب استخدام اتصال الشبكة الافتراضية الخاصة الذي توفره الدار للتعليم فقط للاتصال بأنظمة الخدمات الرقمية والتقنية المدرسية. ويقتد استخدام الطلاب للشبكات الافتراضية الخاصة في مباني المدرسة أو عبر شبكاتها ما لم يُصرَّح بذلك صراحةً لأغراض تعليمية أو إدارية محددة.
- 3- استخدام النسخ غير المصرح بها من البرمجيات والأجهزة المرخصة
- 1-3 يُمنع منعًا باتًا ما يلي:
- 1-1-3 استخدام نسخ غير مصرح بها من البرمجيات والأجهزة المرخصة (القرصنة / انتهاك حقوق الطبع والنشر وبراءات الاختراع) على أنظمة معلومات الدار للتعليم ونسخ هذه المواد.
- 2-1-3 تخزين أو معالجة أو نقل نسخ غير مصرح بها من البرمجيات والأجهزة المرخصة (القرصنة/انتهاك حقوق الطبع والنشر وبراءات الاختراع).
- 4- استخدام التطبيقات المجانية والمشاركة
- 1-4 لا يُسمح بتنصيب واستخدام البرمجيات المجانية أو المشتركة، سواء جرى تنزيلها من الإنترنت أو الحصول عليها عبر أي وسائط أخرى، على أنظمة معلومات الدار للتعليم إلا بعد الحصول على الموافقة اللازمة، ولن يُسمح للمستخدم بتنصيب هذه البرمجيات بنفسه.
- 2-4 تخضع التطبيقات المجانية والمشاركة للتقييم والاختبار من قبل الدار للتعليم قبل تنصيبها على أنظمة معلوماتها.
- 3-4 يُحظر على المستخدمين تنصيب أي ألعاب على أنظمة معلومات الدار للتعليم.

- 5- استخدام المواد المحمية بحقوق الطبع والنشر والأدوات الرقمية
- 1-5 الاستخدام المسؤول للمواد المحمية بحقوق الطبع والنشر
- 1-1-5 يجب أن يمتثل استخدام المواد المحمية بحقوق الطبع والنشر، بما في ذلك على سبيل المثال لا الحصر الكتب والمقالات والصور ومقاطع الفيديو والمحتوى الرقمي، للمرسوم بقانون اتحادي رقم (38) لسنة 2021 بشأن حقوق المؤلف والحقوق المجاورة.
- 2-1-5 يجب على الطلاب وموظفي المدرسة الحصول على التفويض أو التراخيص المناسبة قبل استخدام المواد المحمية بحقوق الطبع والنشر للأغراض التعليمية أو الإدارية
- 3-1-5 وستقدم الدار للتعليم تدريباً وإرشادات حول الاستخدام العادل، والامتثال لحقوق الطبع والنشر، والإسناد الصحيح للمواد الرقمية والمطبوعة مرة واحدة سنوياً على الأقل.
- 4-1-5 يُمنع منعاً باتاً استنساخ أو توزيع أو تعديل المواد المحمية بحقوق الطبع والنشر دون تصريح، وقد يؤدي ذلك إلى عواقب قانونية وتأديبية.
- 2-5 استخدام الأدوات الرقمية، بما في ذلك الذكاء الاصطناعي (AI)
- 1-2-5 يجب أن يتمشى استخدام الأدوات الرقمية، بما في ذلك الذكاء الاصطناعي والتقنيات الناشئة الأخرى، مع الممارسات الأخلاقية والمسؤولة.
- 2-2-5 يجب مراجعة المحتوى الذي يولده الذكاء الاصطناعي للتأكد من دقته، ويُحظر استخدامه لتزييف الملكية الفكرية أو فبركة الأبحاث أو التحايل على الأعمال والواجبات الأكاديمية.
- 3-2-5 وضعت الدار للتعليم مبادئ توجيهية حول كيفية استخدام أدوات الذكاء الاصطناعي في التعلم والتقييم، بما يضمن أنها تُكْمِل العمل الأصلي للطلاب بدلاً من أن تحل محله.
- 4-2-5 أي إساءة استخدام للذكاء الاصطناعي أو الأدوات الرقمية الأخرى لأغراض أكاديمية خادعة سَتُعَامَل على أنها سوء سلوك أكاديمي وتستوجب إجراءً تأديبياً.
- 3-5 مفاهيم النزاهة الأكاديمية والانتحال
- 1-3-5 يجب على جميع الطلاب وموظفي المدرسة الالتزام بأعلى معايير النزاهة الأكاديمية من خلال ضمان أن جميع الأعمال المقدمة هي من إعدادهم وموثقة بشكل صحيح عند الاقتضاء.
- 2-3-5 يُمنع منعاً باتاً الانتحال، بما في ذلك النسخ، أو الاقتباس غير الصحيح، أو استخدام أعمال الآخرين دون إسناد (سواء كانت مكتوبة أو رقمية أو غير ذلك).
- 3-3-5 طبقت المدارس إجراءات لتوعية الطلاب والموظفين حول الانتحال، وأساليب التوثيق الصحيحة، والسلوك الأكاديمي المسؤول.
- 4-3-5 أي حالات انتحال أو غش أكاديمي تُكتشف ستخضع لإجراء تأديبي. وقد يخضع المستخدمون أيضاً لإجراءات تَقَرُّحها السلطة المعنية.
- 6- إدخال المواد الإباحية
- 1-6 يُمنع منعاً باتاً ما يلي:
- 1-1-6 إدخال مواد إباحية إلى أي بيئة من بيئات أنظمة المعلومات.
- 2-1-6 تخزين أو معالجة أو نقل مواد إباحية على أنظمة معلومات الدار للتعليم من قبل المستخدمين.

- 7- إدخال البرامج التخريبية
- 1-7 يُمنع منعاً باتاً إدخال البرامج التخريبية (مثل الفيروسات، والتعليمات البرمجية ذاتية النسخ) التي تهدف إلى إحداث ضرر متعمد، أو التدخل في عمل الآخرين، أو الوصول غير المصرح به، أو إعاقة الإنتاجية لأنظمة معلومات الدار للتعليم.
- 8- الخصوصية والسرية
- 1-8 يجب على جميع المستخدمين الحفاظ دائماً على خصوصية معلومات العملاء ومعلومات الدار للتعليم. تُعتبر جميع المعلومات المتعلقة بالعملاء والمعلومات الداخلية للدار للتعليم خاصة وسرية، ما لم يُشر إلى خلاف ذلك وفقاً لدليل سياسة الخصوصية للدار للتعليم.
- 2-8 البيانات المخزنة على أنظمة معلومات الدار للتعليم هي ملك للمؤسسة، والمخرجات التي ينشئها مستخدمو الدار للتعليم هي أيضاً ملكية فكرية لها.
- 3-8 تلتزم الدار للتعليم بمشاركة بيانات المستخدم داخلياً وخارجياً عندما يقتضي القانون ذلك وفقاً للتشريعات السارية.
- 9- العمل خارج الموقع
- 1-9 يمكن إخراج أجهزة الكمبيوتر المحمولة والأجهزة المتنقلة خارج الموقع مع مراعاة الضوابط التالية:
- 1-1-9 يجب استخدام اتصال VPN الأمن الذي توفره الدار للتعليم فقط للاتصال بأنظمة الخدمات الرقمية والتقنية المكتبية.
- 2-1-9 يُحظر ترك أنظمة معلومات ووسائط الدار للتعليم التي تُؤخذ خارج الموقع دون رقابة في الأماكن العامة.
- 3-1-9 يجب حمل أجهزة الكمبيوتر المحمولة كأمتعة يدوية عند السفر واتخاذ الاحتياطات اللازمة في المطارات.
- 4-1-9 يجب حماية المعلومات من فقدان أو الاختراق عند العمل عن بعد (على سبيل المثال في المنزل أو في الأماكن العامة).
- 5-1-9 يجب توخي الحذر عند استخدام الأجهزة المحمولة مثل أجهزة الكمبيوتر المحمولة، والهواتف المحمولة، والهواتف الذكية، والأجهزة اللوحية. ويجب حمايتها على الأقل بكلمة مرور أو رقم تعريف شخصي (PIN)، وباستخدام التشفير حيثما كان متاحاً.
- 10- الإجراءات عند إنهاء العقد أو ترك المدرسة
- 1-10 يجب إعادة أنظمة معلومات وبيانات الدار للتعليم، مثل أجهزة الكمبيوتر المحمولة والأجهزة المحمولة بما في ذلك الهواتف والهواتف الذكية وأجهزة ذاكرة USB وأقراص CD/DVD (إن وجدت)، إلى الدار للتعليم عند إنهاء العقد/العمل أو عند ترك المدرسة.
- 2-10 تظل بيانات الدار للتعليم أو الملكية الفكرية التي طُورت أو اكتسبت خلال فترة العمل/التعاقد ملكاً للدار للتعليم، ويُحظر الاحتفاظ بها بعد إنهاء العمل/التعاقد مع الدار للتعليم أو إعادة استخدامها لأي غرض آخر.
- 11- استخدام الإنترنت
- 1-11 نظراً لأن خدمات الإنترنت تمثل وسيلة اتصال ونقطة دخول رئيسية إلى العالم الخارجي للدار للتعليم، تقع على عاتق كل مستخدم مسؤولية ضمان استخدام هذه الخدمات بشكل ملائم ومتسق مع هذه السياسة لتسهيل حماية الدار للتعليم من تهديدات الوصول غير المصرح به، وسرقة المعلومات، وسرقة الخدمات، والتعطيل الخبيث للخدمات.
- 2-11 يُعد الوصول إلى الإنترنت عبر شبكة الشركة امتيازاً. يجب على المستخدمين الممنوحين هذا الامتياز الالتزام بالإرشادات الصارمة التالية المتعلقة بالاستخدام الملائم لمورد المعلومات هذا:
- 1-2-11 لا يجوز إلا للموظفين المصرح لهم إنشاء اتصالات بالإنترنت أو بشبكات خارجية أخرى من داخل الدار للتعليم / المدارس

بموافقة إدارة الخدمات الرقمية والتقنية.

2-2-11 يجب على المستخدمين الراغبين في إنشاء اتصال موثوق مع الدار للتعليم / المدارس للوصول إلى الأنظمة الداخلية الخضوع للمصادقة قبل الوصول إلى الشبكة الداخلية.

3-2-11 سُوِّفَ مرافق الاتصال على كل جهاز حوسبة عن بعد للتواصل عبر اتصال موثوق وآمن ومُصادق عليه.

4-2-11 يُحظر على المستخدمين محاولة تعطيل أو محاولة تجاوز أو التحايل على ترتيبات أمن الإنترنت.

5-2-11 يُحظر على المستخدمين انتهاك هذا الامتياز باستخدام الوصول إلى الإنترنت لأغراض غير لائقة قد تسيء إلى سمعة الشركة.

6-2-11 يجب أن يكون الوصول إلى الإنترنت عبر مزود الخدمة الذي تتعاقد معه الدار للتعليم. كما يُمنع الوصول إلى الإنترنت من مرافق الشركة / المدارس عبر أي وسيلة أخرى.

7-2-11 تشمل مؤشرات انخفاض المخاطر الانتمانية على سبيل المثال لا الحصر ما يلي:

- استخدام شبكات قرين إلى قرين مثل Bit-torrent، وLimewire، وKazaa، وTorrents، أو أي جهاز غير مصرح به لنقل الوسائط/الملفات وتخزينها عبر الإنترنت. يُرجى الرجوع إلى سياسة الاتصالات الخاصة بالدار للتعليم للحصول على تفاصيل حول استخدام حسابات وسائل التواصل الاجتماعي الشخصية.
- استخدام المواقع التي تسهل التحايل على الخوادم الوكيل.
- استخدام المواقع التي تسهل خدمة الصوت عبر بروتوكول الإنترنت (VOIP)، وبث الصوت والفيديو، ما لم تصرح بذلك الدار للتعليم.
- المشاركة في أي أنشطة تدوين قد تسيء إلى صورة الدار للتعليم وسمعتها وشهرتها.

8-2-11 يجب على المستخدمين الذين يرغبون في تحميل أو نشر مواد مملوكة للدار للتعليم على الإنترنت أن يكونوا على دراية بوجود قوانين حقوق النشر والعلامات التجارية والتشهير والقتف والرقابة على الخطاب العام في جميع البلدان. ويجب توخي الحذر لعدم انتهاك أي قوانين قد تكون قابلة للتنفيذ ضد الدار للتعليم.

9-2-11 يُحظر على المستخدمين نشر أو وضع أي مواد خاصة بالشركة على أي جهاز كمبيوتر متاح للجمهور دون إذن كتابي مسبق من فريق التسويق والعلامة التجارية في الدار للتعليم.

10-2-11 يُحظر على المستخدمين ما يلي:

- الوصول إلى أو عرض صور/مستندات إباحية ومواد عنصرية أو إرهابية أو ما شابهها على أي نظام تابع للدار للتعليم.
- أرشفة أو تخزين أو توزيع أو تعديل أو تسجيل مواد إباحية ومواد عنصرية أو إرهابية أو ما شابهها باستخدام شبكة أو موارد الحوسبة الخاصة بالدار للتعليم.

11-2-11 في حال وصول المستخدم إلى موقع يحتوي على مثل هذه المواد، ينبغي عليه إنهاء الاتصال مباشرة، بغض النظر عن نتيجة تقييم الموقع من برامج الفحص أو التقييم السابقة.

12-2-11 طبقت الدار للتعليم تقنية منع تسرب البيانات وتراقب بياناتها التي تُشارك خارجيًا وفقًا لسياسة أمن المعلومات الخاصة بالدار للتعليم.

13-2-11 لا يجوز للمستخدمين تنزيل سوى البرمجيات والبيانات التي لها استخدام مباشر في العمل. كما يجب أن تكون جميع هذه البرمجيات والبيانات مرخصة ومسجلة بشكل صحيح. ويجب استخدام البرامج التي تم تنزيلها بموجب شروط ترخيصها فقط. ولا يجوز لأي شخص لديه وصول إلى مرافق الدار للتعليم استخدامها عن علم لتنزيل أو توزيع برمجيات أو بيانات مقرصنة.

- 3-11 تصبح جميع البرمجيات التي يجري تنزيلها عبر الإنترنت إلى شبكة وأنظمة الدار للتعليم ملكًا للشركة. ويجب على المستخدم فحص أي ملف يُنزله بحثًا عن الفيروسات قبل فتحه أو تشغيله.
- 4-11 يجب نقل الملفات التي تحتوي على بيانات سرية أو خاصة عبر الإنترنت باستخدام قناة نقل الملفات التي توفرها إدارة الخدمات الرقمية والتقنية فقط. وتسري جميع القيود المذكورة بشأن الوصول التفاعلي إلى الإنترنت فيما يتعلق بالمواقع الإباحية أو العنصرية أو الإرهابية وغيرها، على البريد الإلكتروني عبر الإنترنت أيضًا.
- 5-11 توجد ترتيبات أمنية شاملة لحماية الشركة. ويُحظر على الموظفين محاولة تعطيل أو محاولة تجاوز أو التحايل على هذه الترتيبات الأمنية للإنترنت.

12- حماية المعلومات

- 1-12 يُمنع منعًا باتًا إرسال المعلومات الحساسة والسرية عبر الإنترنت ما لم يصرح بذلك مالك المعلومات صراحةً. ويشمل ذلك معلومات مثل:
- 1-1-12 أرقام بطاقات الائتمان الخاصة بالشركة، وأرقام بطاقات الاتصال الهاتفية، وتفاصيل العملاء، وتفاصيل الموظفين، وتفاصيل الطلاب، وتفاصيل مجتمع المدرسة، وكلمات مرور تسجيل الدخول، وغيرها من المعلومات التي يمكن استخدامها للوصول إلى أنظمة الشركة أو معلوماتها أو خدماتها، وما إلى ذلك، ويجب عدم إرسالها عبر الإنترنت بصيغة قابلة للقراءة.
- 2-1-12 مواد الشركة (البرمجيات، والمذكرات الداخلية، وما إلى ذلك) على أي جهاز كمبيوتر متاح للجمهور عبر الإنترنت.
- 3-1-12 الشيفرة المصدرية ما لم يكن معروفًا تحديدًا أنها في النطاق العام.
- 4-1-12 معلومات تكوين الشبكة أو الخادم حول أي جهاز تابع للدار للتعليم إلى مجموعات الأخبار العامة أو القوائم البريدية. ويشمل ذلك عناوين الأجهزة الداخلية وأسماء الخوادم وأنواع الخوادم وأرقام إصدارات البرامج.

13- الإقرارات العامة

- 1-13 يُمنع على المستخدمين الإفصاح عن انتمائهم إلى الدار للتعليم ضمن المناقشات على لوحات الإعلانات، وجلسات المحادثة، وسائر الخدمات الإلكترونية الأخرى.
- 2-13 يُحظر على الموظفين أو موظفي الأطراف الثالثة الذين يستخدمون مرافق الدار للتعليم الكشف علنًا عن معلومات داخلية خاصة بالدار للتعليم عبر الإنترنت قد تؤثر سلبيًا على الدار للتعليم وعلاقاتها بالعملاء وصورتها العامة.
- 3-13 يجب على المستخدمين التأكد من أن المنشورات في القوائم البريدية ومجموعات الأخبار العامة والمواقع ذات الصلة لا تكشف عن تفاصيل التشغيل الداخلي أو البنية التحتية أو الثغرات المحتملة في البنية التحتية لأمن معلومات الدار للتعليم. ويُرجى الرجوع إلى سياسة الاتصالات الخاصة بالدار للتعليم للحصول على تفاصيل حول إرشادات وسائل التواصل الاجتماعي.

14- البريد الإلكتروني

- 1-14 تعد خدمات البريد الإلكتروني عاملاً مُمكنًا رئيسيًا لأعمال الدار للتعليم ويجب على المستخدمين ضمان استخدام هذه الخدمات بشكل ملائم ومتسق مع سياسة أمن المعلومات الخاصة بالدار للتعليم.
- 2-14 استخدام البريد الإلكتروني
- 1-2-14 يقتصر الوصول إلى خدمات البريد الإلكتروني على الموظفين المصرح لهم فقط وفقًا لسياسة أمن المعلومات الخاصة بالدار للتعليم.
- 2-2-14 لا يُسمح بالاستخدام المفرط للبريد الإلكتروني في الاتصالات الشخصية.

3-2-14 يجب أن تتبع رسائل البريد الإلكتروني سياسات الشركة المتعلقة باللياقة والمحتوى الملائم، بما في ذلك القيود التالية:

- نقل أو الاشتراك في أي محتوى غير لائق يكون مسيئاً أو تشهيرياً أو مهدداً للآخرين.
- إرسال بيانات أو رسائل أو صور تتكون من مواد إباحية، أو إهانات عرقية، أو نعوت عنصرية، أو أي شيء يمكن تفسيره على أنه مضايقة أو إهانة أو إساءة للآخرين على أساس العرق أو الدين أو الأصل القومي أو اللون أو الحالة الاجتماعية أو حالة المواطنة أو العمر أو الإعاقة أو المظهر الجسدي.
- إنتاج أو توزيع رسائل بريدية جماعية غير مرغوب فيها (تُعرف أيضاً بالرسائل المتسلسلة أو البريد العشوائي) أو تشغيل عمل تجاري أو تقديم طلبات لتحقيق مكاسب شخصية أو لأسباب سياسية أو دينية أو لمنظمات خارجية.
- يُحظر على المستخدمين إعادة توجيه أو نشر الرسائل المتسلسلة أو المخططات الهرمية أو أي أنواع أخرى من البيانات التي قد تستهلك موارد النظام دون داعٍ أو تتدخل في عمل الآخرين إلى الأفراد أو المجموعات.
- نقل أو استلام أسرار تجارية أو مواد محمية بحقوق الطبع والنشر أو معلومات مملوكة أو سرية، ما لم تسمح بذلك شروط استخدام هذه المستندات.

4-2-14 يجب استخدام إخلاءات المسؤولية القانونية والتوقيعات البريدية القياسية في جميع رسائل البريد الإلكتروني. ويُمنع منعاً باتاً إجراء أي تعديلات عليها.

5-2-14 يجب على الموظفين توخي نفس الحذر في صياغة البريد الإلكتروني كما يفعلون في أي مراسلات مكتوبة أخرى تحمل اسم الدار للتعليم.

6-2-14 للحفاظ على الضوابط المناسبة في استخدام خدمات البريد الإلكتروني، يُحظر على المستخدمين الكشف عن معرفات المستخدم وكلمات المرور الخاصة بهم لأي شخص. ويجب على المستخدمين اتخاذ الاحتياطات المناسبة لمنع الاستخدام غير المصرح به لحساب البريد الإلكتروني الخاص بهم، مثل استخدام كلمات مرور معقدة وعدم تدوين كلمات مرور البريد الإلكتروني للرجوع إليها. وترد ضوابط مفصلة لإدارة كلمات المرور في سياسة أمن المعلومات الخاصة بالدار للتعليم.

7-2-14 يُمنع انتحال الشخصية عبر البريد الإلكتروني منعاً باتاً. كما يُحظر على المستخدمين استخدام أسماء مستعارة أو تحريف هوياتهم عبر بريدهم الإلكتروني. ويجب على المستخدمين التعريف بأنفسهم بأسمائهم الحقيقية؛ ويُحظر استخدام أسماء مستعارة لا يمكن نسبتها بسهولة إلى المستخدمين الفعليين.

8-2-14 يُمنع منعاً باتاً تزوير معلومات الترويسة في رسالة بريد إلكتروني. ويشمل ذلك تغيير عنوان المصدر وعنوان الوجهة والطابع الزمنية.

9-2-14 يُحظر على المستخدمين نشر أو توزيع القوائم البريدية الداخلية على أطراف خارجية.

10-2-14 يُحظر فتح المرفقات من مصادر غير معروفة أو غير موثوقة. ويجب على المستخدمين فحص مرفقات البريد الإلكتروني، بغض النظر عن المصدر أو المحتوى، بحثاً عن الفيروسات والبرامج التخريبية الأخرى قبل فتحها أو تخزينها على أي نظام كمبيوتر تابع للدار للتعليم. يجب الإبلاغ عن أي مصدر غير موثوق به أو رسائل بريد إلكتروني يُشتبه في أنها ضارة إلى مكتب خدمة الدار للتعليم (sd@aldareducation.com).

3-14 يُحظر على الموظفين أو الأفراد أو الطلاب أو مقاولي الأطراف الثالثة الذين يستخدمون مرافق الدار للتعليم تعديل معايير الأمان داخل نظام البريد الإلكتروني. ويعتبر المستخدمون الذين يجرون تغييرات غير مصرح بها على معايير أمان البريد الإلكتروني مخالفين لهذه السياسة.

4-14 سيحظر نظام البريد الإلكتروني أحجام ملفات المرفقات التي تزيد على 35 ميغابايت لمنع استهلاك النطاق الترددي على حساب المستخدمين الآخرين. كما سترسل إشعارات الخطأ تلقائياً عن رسائل البريد الإلكتروني التي لم تُسلم إلى المرسل. ويُحظر إرسال رسائل

بريد إلكتروني لا تتعلق بالعمل وتحتوي على مرفقات ملفات كبيرة، مثل ملفات الرسومات والوسائط المتعددة.

5-14 يُحظر على المستخدمين تنفيذ أي برامج مستلمة عبر البريد الإلكتروني. ويُحظر على المستخدمين تثبيت أي ترقيات أو تصحيحات مستلمة عبر البريد الإلكتروني.

6-14 بموافقة مسبقة، يجوز للدار للتعليم في أي وقت وبإشعار أو بدونه، مراقبة هذه المعلومات أو البحث فيها أو مراجعتها أو الكشف عنها أو اعتراضها لأي غرض مشروع، بما في ذلك على سبيل المثال لا الحصر ما يلي:

1-6-14 مراقبة الأداء.

2-6-14 ضمان الامتثال لسياسات الدار للتعليم.

3-6-14 منع إساءة استخدام خدمات البريد الإلكتروني.

4-6-14 استكشاف مشكلات الأجهزة والبرامج وإصلاحها.

5-6-14 الامتثال للطلبات القانونية والتنظيمية للحصول على المعلومات.

6-6-14 التحقيق في الكشف عن معلومات تجارية سرية أو مملوكة أو سلوك قد يكون غير قانوني أو يؤثر سلبًا على الدار للتعليم أو شركائها.

15- مكافحة الفيروسات

1-15 يجب على المستخدمين الامتثال لسياسة أمن المعلومات الخاصة بالدار للتعليم والتدابير المطبقة للحماية من البرامج الضارة، المعروفة باسم فيروسات الكمبيوتر.

2-15 اعتمادًا على طبيعة الفيروس، قد يكون له تأثير طفيف أو كبير على سلوك النظام أو أدائه، أو قد يؤدي إلى فقدان البيانات أو سرية المعلومات، بل وحتى فقدان الثقة أو السمعة من عملائنا وشركائنا التجاريين.

3-15 مسؤوليات المستخدمين هي كما يلي:

1-3-15 يجب على المستخدمين دائمًا تشغيل برنامج مكافحة الفيروسات القياسي الذي توفره الدار للتعليم. وتسلم جميع أجهزة الكمبيوتر (المكتبية والمحمولة) مع تثبيت مسبق لبرنامج مكافحة الفيروسات القياسي.

2-3-15 يُحظر على المستخدمين محاولة تغيير أو تعطيل برنامج مكافحة الفيروسات المثبت على أي جهاز كمبيوتر متصل بالشبكة.

3-3-15 إذا استلم مستخدم ما يعتقد أنه فيروس، أو اشتبه في إصابة جهاز كمبيوتر بفيروس، فيجب عليه إبلاغ مكتب خدمة الدار للتعليم (sd@aldareducation.com) فورًا. ويجب تقديم المعلومات التالية، إن كانت معروفة: اسم الفيروس، ومدى الإصابة، ومصدر الفيروس، والمستلمين المحتملين للمواد المصابة.

4-3-15 يجب على المستخدمين الامتناع عن القيام بالإجراءات التالية:

- محاولة تدمير أو إزالة فيروس، أو أي دليل على وجود ذلك الفيروس، دون توجيه من إدارة الخدمات الرقمية والتقنية.
- إعادة توجيه هذه الرسائل أو أي رسائل تحذير من الفيروسات عبر البريد الإلكتروني للحفاظ على حركة مرور الشبكة عند الحد الأدنى.

- فتح أي ملفات أو وحدات ماكرو مرفقة برسالة بريد إلكتروني من مصدر غير معروف أو مشبوه أو غير موثوق.
- فتح أي ملفات أو وحدات ماكرو مرفقة برسالة بريد إلكتروني من مصدر معروف (حتى لو كان زميل عمل) إذا لم تكن تتوقع مرفقًا معيّنًا من ذلك المصدر.

- النقر على رابط أرسل إلى المستخدم إذا لم يكن يتوقع رابطًا معيّنًا. ويجب على المستخدمين الشك في رسائل البريد الإلكتروني التي تحتوي على روابط لمواقع ويب غير معروفة. من المحتمل أن يكون الرابط ملفًا تنفيذيًا ضارًا (exe.) متخفيًا في شكل رابط.

- نسخ أو تنزيل أو تثبيت ملفات من مصادر غير معروفة أو مشبوهة أو غير موثوقة.

5-3-15 تحظر خدمات الفحص والمراقبة الخارجية الملفات ذات امتدادات معينة، والتي تشمل الملفات ذات الامتدادات *.BAT، و*.EXE، و*.SYS. يجب على المستخدمين الاتصال بمكتب خدمة الدار للتعليم (sd@aldareducation.com) للحصول على المشورة إذا كانوا بحاجة إلى ملف مذكور أعلاه.

4-15 يجب على المستخدم تجنب قدر الإمكان - مشاركة الأقراص الصلبة الخارجية التي لها صلاحية القراءة/الكتابة. ويجب على المستخدمين دائمًا فحص الوسائط القابلة للإزالة بحثًا عن الفيروسات قبل استخدامها. إذا استخدمت أجهزة الكمبيوتر المنزلية المملوكة شخصيًا لأغراض العمل ونُقلت الملفات إلى كمبيوتر العمل، فيجب على المستخدم التأكد من فحص الوسائط والملفات قبل الاستخدام.

5-15 الحماية من الفيروسات والبرامج الضارة

1-5-15 يُمنع منعًا باتًا إدخال البرامج التخريبية (مثل الفيروسات، والتعليمات البرمجية ذاتية النسخ) التي قد تسبب ضررًا متعمدًا، أو تتدخل في عمل الآخرين، أو تتيح الوصول غير المصرح به، أو تعيق الإنتاجية لأنظمة معلومات الدار للتعليم.

2-5-15 ستزيل الدار للتعليم أي جهاز كمبيوتر يُعتقد أنه مصاب بفيروس من الشبكة حتى يتم التحقق من خلوه من الفيروسات.

16- تخزين البيانات على ONEDRIVE / SHAREPOINT

1-16 تخضع مساحة تخزين خادم الملفات لإدارة قسم الخدمات الرقمية والتقنية لضمان التوافر المستمر لمساحة التخزين على الشبكة.

2-16 مجلد المستخدم (OneDrive / SharePoint): توفر الدار للتعليم لكل مستخدم وصولاً آمنًا إلى OneDrive / SharePoint كجزء

من اشتراك مايكروسوفت أوفيس 365 للتخزين المخصص على السحابة مع وصول مقيد بذلك المستخدم. ويجب على المستخدم الحفاظ على التنظيم الجيد لمجلدات OneDrive / SharePoint الخاصة به والتأكد من إزالة الملفات الزائدة التي لم تعد هناك حاجة إليها.

3-16 يجب على المستخدمين استخدام OneDrive / SharePoint كمخزن أساسي للنسخ الإلكترونية من مستندات العمل. ويجب أن يتوافق استخدام نظام تخزين البيانات مع هذه السياسة. تشمل الملفات غير الملائمة ملفات MP3 غير المتعلقة بالعمل، وملفات GIF، والألعاب، والملفات التنفيذية، وملفات VBS، وأي برامج أخرى يثبتها المستخدم ولم توافق عليها الدار للتعليم.

17- المراسلة الفورية

1-17 تُستخدم المراسلة الفورية عبر مايكروسوفت تيمز حاليًا كشكل من أشكال الاتصال الفوري بين الموظفين. وتهدف تقنية المراسلة الفورية إلى تعزيز الإنتاجية أثناء تسيير الأعمال.

1-1-17 الاستخدام المقبول: يجب استخدام خدمات المراسلة الفورية للاتصالات التجارية ولأداء الواجبات الوظيفية، وفقًا لأهداف

وغايات الشركة. يجب على المستخدمين ممارسة التقدير السليم والحس السليم أثناء استخدام المراسلة الفورية لأداء واجباتهم

الوظيفية. يعد استخدام المراسلة الفورية امتيازًا، ولا يُقبل إساءة استخدامه أو استغلاله؛ ويجب الالتزام بسياسة الاستخدام

المسؤول لأنظمة المعلومات عند استخدام المراسلة الفورية.

2-1-17 الاستخدام الشخصي: لا يجوز للمستخدمين استخدام خدمة المراسلة الفورية الخاصة بشركة الدار للتعليم لأسباب شخصية

خلال ساعات العمل العادية.

3-1-17 الاستخدام غير المقبول: يجب عدم استخدام خدمة المراسلة الفورية لأغراض قد يُتوقع بشكل معقول أن تسبب ضغطًا مفرطًا

على الأنظمة، مثل:

• عرض أو نسخ أو تغيير أو حذف حسابات أو ملفات المراسلة الفورية الخاصة بشركة أخرى أو فرد آخر دون إذن

مصرح به.

• مشاركة كلمات مرور حساب المراسلة الفورية مع شخص آخر أو محاولة الحصول على كلمة مرور حساب المراسلة

الفورية لشخص آخر. يجب أن يستخدم المستخدم المسجل فقط حسابات المراسلة الفورية.
• الاستخدام الشخصي المفرط لموارد المراسلة الفورية.

- 4-1-17 السرية: لا يُشجع على نقل المعلومات الحساسة للشركة عبر المراسلة الفورية لأغراض العمل. ويُحظر على المستخدمين إرسال معلومات شخصية أو مسائل سرية أو معلومات أخرى مملوكة عبر خدمة المراسلة الفورية الخاصة بالشركة.
- 5-1-17 تُعتبر محادثات ورسائل المراسلة الفورية التي تُنشأ على خدمة المراسلة الفورية الخاصة بالشركة وتُنقل عبر أنظمة الشركة ملوكًا للدار للتعليم. ورغم أن هذه المحادثات لا تُسجل، تحتفظ الدار للتعليم بالحق في تسجيل ومراقبة وفحص ونسخ ومراجعة وتخزين وتدقيق استخدام المراسلة الفورية والرسائل التي تُنشأ من قبل المؤسسة أو لها. ويجب ألا يتوقع المستخدمون وجود خصوصية بشكل معقول عند استخدام خدمات المراسلة الفورية الخاصة بالشركة.
- 6-1-17 مشاركة ملف: لا يُشجع على مشاركة الملفات الخارجية عبر خدمات المراسلة الفورية. توفر الدار للتعليم وسائل أخرى معتمدة لنقل الملفات مثل البريد الإلكتروني، ومجلد الخادم المشترك، وOneDrive، وSharePoint، وخدمة FTP.

18- العناية الواجبة

- 1-18 تقع على عاتق كل مستخدم مسؤولية إخطار مكتب خدمة الدار للتعليم (sd@aldareducation.com) فورًا بأي دليل أو اشتباه في أي انتهاك أمني يتعلق بما يلي:
- 1-1-18 الوصول غير المصرح به إلى الشبكة أو الاتصالات السلكية واللاسلكية أو أنظمة الكمبيوتر.
- 2-1-18 الوجود الواضح لفيروس أو برنامج ضار على نظام صادر عن الشركة.
- 3-1-18 الوجود الواضح لأي مادة غير لائقة تحظرها هذه السياسة.
- 4-1-18 العبث الواضح بأي ملف فرض عليه المستخدم ضوابط وصول مقيدة.
- 5-1-18 انتهاك هذه السياسة أو أي سياسات أو إجراءات أخرى لأمن المعلومات من قبل مستخدم آخر.
- 2-18 يجب على المستخدم منع الوصول غير المصرح به، بما في ذلك العرض، إلى موارد المعلومات أو المواد التي في حوزته أو تحت سيطرته أو عهده.

ج- التعريفات

المصطلح أو الاختصار	التعريف
الدار للتعليم أو الشركة	يشير إلى الدار للتعليم بما في ذلك جميع مدارس الدار للتعليم المشغلة، والمدارس المُدارة، وأكاديمية الدار للتدريب.
AI	الذكاء الاصطناعي.
أكاديمية الدار للتدريب	تشير إلى أكاديمية الدار للتدريب التي تديرها الدار للتعليم.
/	تعني "أو" وتُستخدم لربط البدائل.
CD	قرص مضغوط.

الإدارة	وحدة تنظيمية في الشركة، تشكل جزءاً من قسم. وتقع الإدارة تحت قيادة منصب رئيس أو أعلى، يتبع مباشرة للمدير التنفيذي للقسم.
بأقة السلامة الرقمية	تشير إلى التدابير والضوابط الأمنية المصممة لضمان الاستخدام الآمن والمسؤول للأجهزة الرقمية وشبكة الدار للتعليم.
القسم	وحدة تنظيمية رأسية في الشركة، تقع تحت قيادة مدير تنفيذي يتبع مباشرة للرئيس التنفيذي، وقد يكون لها إدارات تابعة.
DTS	الخدمات الرقمية والتقنية
DVD	قرص فيديو رقمي.
الموظف	يشمل الموظفين المؤقتين والدائمين والعاملين بدوام كامل وجزئي.
الهيكل	نوع متخصص من السياسات يحتوي على هيكل منطقي يُصمم لتنظيم وثائق أخرى في خطة أو تسلسل هرمي أو هيكل.
FTP	بروتوكول نقل الملفات.
الوظيفة	منطقة تشغيلية داخل الإدارة، كما هو محدد في هيكلها التنظيمي.
GIF	تنسيق تبادل الرسومات.
الوثيقة الحاكمة	الوثيقة الحاكمة هي أي مستند يرسخ القواعد أو المبادئ أو الإرشادات التي يجب أن تتماشى معها السياسة/إطار العمل.
HQ	المقر الرئيسي.
IM	التراسل الفوري
الوثيقة	وثيقة لتقديم التوجيه، أو فرض الالتزامات، أو تحديد المسؤوليات، أو تفويض السلطات، مثل إطار العمل، والسياسة، وإجراءات التشغيل القياسية، وما إلى ذلك.

المصطلح أو الاختصار	التعريف
IP	بروتوكول الإنترنت هو بروتوكول لإرسال البيانات عبر الشبكات باستخدام عناوين بروتوكول الإنترنت.

المدارس المُدارة	تشير إلى مدارس أدنوك أو دائرة التعليم والمعرفة التي تديرها الدار للتعليم. وتخضع مجالات المسؤوليات المحددة للاتفاقيات القانونية ذات الصلة المبرمة مع هذه الكيانات.
MDM	إدارة أجهزة الهاتف الجوال
MP3	طبقة الصوت MPEG 3 هو تنسيق تشفير صوتي رقمي يستخدم ضغط البيانات لتقليل حجم الملفات الصوتية.
المدارس المُشغلة	تشير إلى المدارس المملوكة بالكامل والمشغلة مباشرة من قبل الدار للتعليم.
دليل السياسات والإجراءات	وثيقة تحتوي على بيانات المبادئ، أو قواعد العمل، أو الضوابط الداخلية المصاغة والمتوافقة مع المتطلبات القانونية أو التنظيمية أو التنظيمية، والتي تسترشد بها الدار للتعليم في إدارة شؤونها وتطوير
الإجراء / إجراء التشغيل القياسي (SOP)	وثيقة تصف الأنشطة اللازمة لتنفيذ سياسة ما، وتركز على المسؤوليات والمتطلبات اللازمة لإنجاز المهام والأنشطة والعمليات.
العملية	سلسلة من المهام التي يتعين القيام بها لإنجاز المهام التشغيلية، وتحقيق النتائج أو المخرجات المرجوة في نهاية المطاف، والمساهمة في التشغيل الناجح للشركة. وتحدد العملية أيضاً مسؤوليات محددة ووثائق داعمة ضرورية لتنفيذها وصيانتها بالكامل.
PIN	رقم التعريف الشخصي.
المستندات الداعمة	المستندات التي تدعم تنفيذ الوثائق. تشمل المستندات الداعمة على سبيل المثال لا الحصر المبادئ التوجيهية، والنماذج، والقوالب، وإجراءات التشغيل القياسية، أو أي وثائق "غير خاضعة للرقابة" (مثل التي يُنشئها النظام أو الوثائق الخارجية).
المستخدم / المستخدم (المستخدمون) النهائيون	يُعرّف المستخدم النهائي، في سياق تقنية المعلومات، بأنه المستهلك أو المستخدم النهائي الأخير لمنتج أو نظام أو خدمة والمستخدمون النهائيون هم أفراد يتفاعلون مباشرة مع تطبيق البرنامج النهائي أو الجهاز أو الخدمة الرقمية، مستخدمين ميزاتها ووظائفها لتلبية احتياجاتهم أو متطلباتهم الخاصة.
	بالنسبة للدار للتعليم، قد يشير هذا إلى الموظفين عبر الدار للتعليم ومدارسها، والمقاولين، والطلاب، وأولياء الأمور، بالإضافة إلى أي أفراد أو كيانات أخرى قد تستخدم موارد المعلومات وتقنية المعلومات التابعة للدار للتعليم.
USB	الناقل التسلسلي العام هو منصة شائعة تسمح بالاتصال بين الأجهزة ووحدة تحكم مضيفة مثل الكمبيوتر.
VBS	نص فيجوال بيسك.
VoIP	الصوت عبر بروتوكول الإنترنت.

المصطلح أو الاختصار	التعريف
VPN	شبكة خاصة افتراضية