COGNITA

Europa

Política Regional de TI

Septiembre 2024

Versión para España

Contenidos

1 Introducción

El uso de la tecnología como herramienta facilitadora del aprendizaje se ha convertido en parte integral de la vida escolar y familiar. Cognita se compromete a utilizar la tecnología de forma eficaz y útil para la enseñanza, el aprendizaje y la administración, y se compromete plenamente a proteger a su personal (incluyendo el personal interno y externo), al alumnado, a las familias y a los visitantes, colectivamente "las partes interesadas", frente al uso ilegal o perjudicial de la tecnología por parte de individuos o grupos, ya sea con o sin ánimo de hacerlo.

Cognita promueve activamente la participación de las familias para ayudar al centro a salvaguardar el bienestar de los/las alumnos/as y fomentar el uso seguro de la tecnología.

Esta política aplica al uso de equipos, aplicaciones y servicios informáticos denominados colectivamente "tecnología" (tanto dentro como fuera del centro) que se suministran y/o se ponen a disposición de las partes interesadas a través de los colegios y/o de las oficinas regionales.

Se puede solicitar una copia física de esta política, que también está disponible en el sitio web del centro.

En caso de incumplimiento de esta política, no se aceptará como defensa el hecho de no haberla leído. En tales casos, Cognita se reserva el derecho a investigar y adoptar las medidas necesarias.

2 Objetivo de la política

2.1 Promover una cultura de comportamiento responsable, uso seguro y cuidado de la tecnología a disposición de las partes interesadas, tanto en los centros escolares como en las oficinas regionales (dentro o fuera de las instalaciones).

2.2 Describir el uso aceptable e inaceptable de la tecnología en los colegios y oficinas regionales (tanto dentro como fuera de las instalaciones).

2.3 Describir las principales funciones y responsabilidades de todas las partes interesadas en el uso de la tecnología Cognita.

2.4 Educar y animar a los/las alumnos/as para que hagan un buen uso de las oportunidades educativas que ofrece el acceso a la tecnología en sus centros educativos.

2.5 Salvaguardar y promover el bienestar de los/las alumnos/as, en particular, anticipando y previniendo los riesgos derivados de:

- Exposición deliberada o involuntaria a contenidos nocivos y/o inapropiados como contenido pornográfico, racista, extremista y/u otros contenidos ofensivos.
- Contacto inapropiado con personas adultas conocidas fuera de la escuela y/o con personas desconocidas
- Conducta inapropiada cuando se usa la tecnología
- Ciberacoso y/o abuso online
- Copia y compartición de datos personales
- Preocupaciones y riesgos relacionados con el comercio; por ejemplo, fraude, estafa y/o extorsión.

2.6 Describir el proceso y los requisitos para informar sobre el uso indebido de la tecnología y los incidentes.

2.7 Garantizar que todas las partes interesadas disponen de las medidas necesarias para mantenerse a salvo y seguras.

3 Aplicación de la política

3.1 Esta política aplica a todas las partes interesadas en las escuelas y oficinas de Cognita.

3.2 Los centros escolares adoptarán un enfoque amplio e intencionado a la hora de considerar qué se entiende por tecnología. Esta política se refiere a todos los dispositivos tecnológicos, informáticos y de comunicaciones, el hardware de red, el software y los servicios asociados a ellos, incluidos, entre otros, los siguientes:

- La red escolar, WIFI y acceso a Internet
- Hardware y dispositivos digitales, incluidos los dispositivos "inteligentes"
- Software (basado en la nube y local)
- Aplicaciones de comunicación y colaboración (por ejemplo, correo electrónico, Microsoft Teams, WhatsApp, Snapchat)
- Entornos virtuales de aprendizaje
- Redes sociales (por ejemplo, Facebook, Instagram, Tik Tok, X - antes Twitter)

Esta política aplica a cualquier miembro de la comunidad escolar cuyo comportamiento o acciones pongan en peligro la cultura o la reputación de la escuela o de las partes interesadas.

4 Roles y responsabilidades

Esta política es responsabilidad del Responsable de TI de Cognita Europa y Norteamérica, quien garantizará que la tecnología se implante y supervise de acuerdo con esta política, así como con otras políticas pertinentes.

4.1. Los/las Directores/as Generales de los PODs (Reino Unido), los/as Directores/as Generales (España, Italia y Suiza) y los/las Directores/as de los centros educativos son responsables de la publicación de esta política y de su aplicación y supervisión continuas a nivel de centro educativo.

4.2. Todas las partes interesadas son responsables del cumplimiento de esta política.

4.3. El Responsable de Ciberseguridad es responsable de los servicios cibernéticos, así como del proceso de filtrado y supervisión.

4.4. El Responsable de Protección de Menores (DSL), conocido como Coordinador/a de Bienestar y Protección (CPC) en España, es la persona responsable (con el apoyo delegado de los adjuntos y/o personal de TI) de tener una visión general de la protección y la seguridad online. Esto incluye (pero no se limita a):

- Supervisar la actividad online de los/las alumnos/as y llevar un registro de la misma (más información en el Apéndice A - Declaración sobre el filtrado de páginas web).
- Realizar un seguimiento de los problemas de protección relacionados con la comunicación digital o todos los asuntos informáticos que afecten a los/las alumnos/as, a sus familias y/o tutores legales y a organismos externos, según proceda (más información en la Política de Protección Integral del Menor de Cognita).

- Plantear cualquier problema complejo relacionado con los dispositivos de control y/o sus resultados en relación con alumnos/as a la Responsable Regional de Protección de Menores (quien, en caso necesario, remitirá la cuestión al Responsable Europeo de TI si se trata de un problema relacionado con la tecnología).
- Asegurarse de que el personal está formado en seguridad online de los/las alumnos/as y cómo reconocer los riesgos e indicadores que puedan generar preocupación.
- Asegurarse de que se le enseña al alumnado cómo mantenerse seguro online y acerca de los potenciales riesgos de la actividad online.

5 Uso seguro de la tecnología

5.1 La escuela está comprometida con el uso seguro y útil de la tecnología para la enseñanza, el aprendizaje y la administración.

5.2 El uso de la tecnología debe ser seguro, responsable, respetuoso con los demás y ceñirse a la legalidad. Las partes interesadas son en todo momento responsables de sus acciones, conducta y comportamiento al utilizar la tecnología.

5.3 La escuela apoyará el uso de la tecnología y hará que las restricciones en el acceso a Internet sean proporcionadas, equilibrando al mismo tiempo las necesidades educativas, la seguridad y el bienestar de las partes interesadas pertinentes, así como la seguridad y la integridad de nuestros sistemas.

5.4 Disponemos de herramientas de supervisión, registro y alerta para mantener la seguridad tecnológica y la protección de las partes interesadas.

5.5 Las herramientas de filtrado y supervisión se revisan anualmente de forma centralizada para garantizar que las disposiciones actuales satisfacen todas las necesidades de nuestro personal y nuestros/as alumnos/as. En esta revisión participan integrantes de los equipos de TI, Ciberseguridad, y Protección del Menor, así como los Gobernadores y Propietarios.

5.6 En aras de la protección de los/las menores, los dispositivos 1 a 1 de los/las alumnos/as tienen preinstalado un software de supervisión que bloquea determinados sitios y proporciona datos en tiempo real e históricos sobre el uso del dispositivo, por ejemplo, la navegación web. Los datos recogidos se almacenan durante un periodo máximo de 90 días.

5.7 El software de supervisión utiliza Inteligencia Artificial (IA) para determinar cómo se filtran los nuevos sitios web y a qué categorías pertenece su contenido (más detalles en el Apéndice A).

5.8 Los equipos de Soporte y la Dirección de Informática tienen autoridad para realizar cambios manuales en el sistema de filtrado de los centros escolares, siempre que cuenten con la aprobación del equipo directivo del centro y/o del Departamento Regional de Informática.

5.9 El equipo de protección del menor de los centros escolares es responsable de supervisar los sistemas y procesos de control establecidos. Los equipos de protección del menor del centro supervisan periódicamente el uso que hacen los/las alumnos/as de los dispositivos del centro, dando prioridad a los/as alumnos/as vulnerables y realizando controles aleatorios siempre que sea posible desde el punto de vista operativo. Hay formación disponible para ayudar al personal a entender cómo analizar los datos de filtrado dentro del sistema Lightspeed.

5.10 Todo el personal, y aquellos con responsabilidad de gobernanza, reciben formación anual sobre la ciberseguridad.

5.11. Todo el personal debe entender las expectativas y responsabilidades relacionadas con el sistema de filtrado. Todo el personal debe ser consciente de que el sistema de filtrado tiene por objeto proteger al alumnado de contenidos online nocivos, incluidos los relacionados con la pornografía y los contenidos para adultos, la radicalización, la violencia, el odio y el racismo, las actividades delictivas y el terrorismo*. La idoneidad de los sistemas de filtrado y supervisión es competencia de cada centro escolar y se basará, en parte, en la evaluación de riesgos exigida por el Deber de Prevención (Reino Unido), en consonancia con la estrategia del Gobierno del Reino Unido para impedir que las personas se conviertan en terroristas y/o apoyen el terrorismo.

5.12. El centro escolar puede solicitar que se introduzcan cambios a medida en el sistema de filtrado para su centro, y deberá solicitarlo a través del Servicio de Atención al Usuario de Cognita o del Responsable de TI del centro.

5.13. Queremos que los/las alumnos/as disfruten utilizando la tecnología y que se conviertan en usuarios expertos, ya que la tecnología se ha convertido en una parte fundamental de la educación, no sólo como vehículo para impartir una enseñanza y un aprendizaje excelentes, sino también como plataforma para la colaboración y la productividad.

5.14. Es responsabilidad de cada colegio educar a su alumnado acerca de la importancia del uso seguro y responsable de la tecnología para ayudar a protegerse a sí mismos y a los demás mientras estén online. El equipo regional de TI apoya esto a través de diversos recursos y políticas (incluida ésta).

5.15. Cognita fomenta los comentarios y la participación de las familias, por ejemplo, a través de la encuesta «Voice of the Parent» (VoP), para ayudar a promover el uso seguro de la tecnología por parte de los/las alumnos/as.

5.16. Cualquier preocupación relacionada con el uso inseguro o inadecuado de la tecnología debe comunicarse a un miembro del Equipo de Liderazgo, al/a la Director/a del centro, al DSL/CPC o al Service Desk de Cognita el mismo día en que se detecte esa preocupación.

5.17. El/la Director/a del centro y/o el DSL/CPC deben informar inmediatamente de cualquier incidente grave relacionado con el uso inseguro o inadecuado de la tecnología al Responsable de TI de Cognita Europa y EEUU (para asuntos tecnológicos) y a la Responsable Regional de Protección de Menores (para asuntos de protección de menores), quienes colaborarán con los/las compañeros/as pertinentes para registrar, investigar y mitigar los riesgos relacionados con el incidente. El colegio deberá cumplimentar un Formulario de Incidente Serio (SIRF), tras su investigación e intervenciones con el apoyo de la Dirección Regional de TI y Protección del Menor.

5.18. Todos los usuarios de tecnología pueden encontrar los siguientes recursos útiles para mantenerse a sí mismos y a otros seguros mientras estén online:

- UK Safer Internet Centre
- Internet Matters - resources
- Google Family Safety
- Common Sense Media

Además, los centros escolares deben tener en cuenta la necesidad de cumplir las normas de ciberseguridad establecidas por las autoridades locales y nacionales.

Para ayudar a los centros a cumplir esta obligación, el Ministerio de Educación (UK) ha publicado una serie de normas de filtrado y supervisión que establecen que los centros deben:

- Identificar y asignar funciones y responsabilidades para gestionar los sistemas de filtrado y supervisión.
- Revisar los sistemas de filtrado y control al menos una vez al año
- Bloquear los contenidos nocivos o inadecuados (por ejemplo, imágenes explícitas, contenidos violentos o que inciten al odio y otras formas de medios nocivos) sin que ello afecte injustificadamente a la enseñanza y el aprendizaje.
- Disponer de estrategias de supervisión eficaces que respondan a sus necesidades de protección.

6 Derecho a utilizar equipamiento y redes del colegio u oficina

6.1 A todo el personal y a los/las alumnos/as de los colegios se les asignará un nombre de usuario y una contraseña para acceder a los dispositivos y servicios tecnológicos. No deben permitir que otras personas utilicen su cuenta y no compartirán ninguna contraseña con nadie.

6.2 Solo se debe acceder a las cuentas de correo electrónico del colegio a través de los entornos Microsoft Office 365 o Google de Cognita. No se permiten todos los demás servicios de correo electrónico de terceros.

6.3 Algunos recursos compartidos (disponibles en el colegio y en las oficinas para uso de personal y alumnos/as) tendrán un nombre de usuario y contraseña genéricos para su acceso y es gestionado por el profesorado.

6.4 Toda la tecnología del centro educativo seguirá siendo propiedad de Cognita. El centro podrá solicitar razonablemente el dispositivo o retirar el acceso al servicio, a cualquier alumno/a, en cualquier momento y, en su caso, el dispositivo deberá ser devuelto al centro por el alumno/a.

6.5 Sólo los dispositivos que sean propiedad del colegio deben conectarse a la red del centro y los dispositivos personales sólo deben conectarse a la red de invitados, siempre que lo permita un miembro del Equipo de Liderazgo del centro.

6.6 Los dispositivos personales del personal educativo o no educativo no deben utilizarse para tareas relacionadas con el trabajo en la escuela y nunca deben utilizarse en presencia de alumnos/as.

6.7 Se prohíbe cualquier intento de acceder o utilizar cualquier cuenta, dirección de correo electrónico o recurso informático que pertenezca a otra parte interesada, a menos que dicho intento sea realizado por el Departamento Regional de Informática por motivos comerciales legítimos y/o haya sido autorizado mediante el formulario de solicitud de acceso Access to Mailbox and Files Request Form.

6.8 Los dispositivos designados pueden ser entregados a los/las empleados/as del colegio y a los/las alumnos/as para la enseñanza, el aprendizaje y la administración:

- Los/las alumnos/as asignados/as con un dispositivo 1-to-1 deberán firmar el Acuerdo de Uso del iPad/Laptop (enlace en el Apéndice)
- Los/las alumnos/as con un dispositivo 1-to-1 designado pueden utilizarlo en las clases bajo la dirección del profesorado
- El personal de la escuela y los/las alumnos/as son responsables de la seguridad del dispositivo asignado cuando esté fuera de las instalaciones del centro.
- Los dispositivos proporcionados por la escuela y los periféricos asociados deben ser devueltos en buenas condiciones (excluyendo el desgaste ordinario) y en buen estado de funcionamiento cuando la persona a quien le ha sido entregado el dispositivo sea alumno/a o empleado/a, finalice su relación con el colegio
- Los dispositivos dañados y/o defectuosos del personal se reparan o sustituyen, y los costes son cubiertos de forma centralizada o por la escuela.
- Las familias son responsables del coste de una "reparación" o sustitución "por otro igual" de un dispositivo asignado (según las instrucciones de la escuela), si se daña / pierde intencionadamente, deliberadamente o por negligencia.

7 Uso adecuado de la tecnología para la seguridad digital

7.1 El colegio proporciona **cuentas de sistema y de aplicación** para las partes interesadas con fines educativos y administrativos.

7.2 Las partes interesadas **no deben**:

- Permitir que nadie utilice su cuenta a menos que esté autorizado (por escrito) por el SLT y/o el Equipo Regional de TI.
- Utilizar la cuenta de otra persona
- Dejar su dispositivo desbloqueado y/o conectado a su cuenta cuando no esté en uso.
- Utilizar aplicaciones de mensajería móvil para comunicarse con las familias, así como el personal tampoco debe contactar con los/las alumnos/as.
- Enviar mensajes y/o correos electrónicos desde cuentas del colegio que se hagan pasar por una persona que no es la que realmente envía el mensaje, a menos que lo apruebe un miembro del SLT de la escuela.
- Enviar mensajes y/o correos electrónicos relacionados con el trabajo a/desde una cuenta personal.

7.3 La escuela proporciona **hardware y software** para apoyar la educación y el funcionamiento de la escuela.

- Se espera que los usuarios de los equipos tecnológicos del centro los cuiden con un comportamiento responsable.
- La tecnología del centro no debe ser retirada del recinto escolar excepto cuando:
    - El dispositivo esté asignado a un miembro del personal; o
    - El dispositivo esté asignado a un/a alumno/a a través del programa 1 a 1; o
    - Se cuente con el permiso por escrito de un miembro del Equipo de Liderazgo.

- La tecnología escolar asignada al personal y al alumnado es responsabilidad de la persona a quien ha sido asignada.
- Las partes interesadas **no deben** dejar desatendidos los equipos tecnológicos portátiles, incluidos los dispositivos proporcionados por la escuela, a menos que dichos equipos estén fuera de uso (ya sea debido a avería(s) o simplemente, desconectados y apagados), en cuyo caso, deben guardarse de forma segura.
- La pérdida o daño de la tecnología escolar debe ser reportada a un miembro del personal docente, miembro del SLT o Equipo de Apoyo de TI en el mismo día
- El robo de tecnología escolar asignada a un miembro individual del personal o a un/a alumno/a a través del programa 1-to-1 debe ser denunciado a la Policía y comunicado a un miembro del personal docente o del SLT o al Equipo de Apoyo de TI en el mismo día con el número de referencia del delito de la Policía. En caso de que se produzca en el colegio, el propio colegio hará la denuncia. El uso indebido deliberado o el deterioro de los equipos tecnológicos del centro dará lugar a que se facturen a la(s) persona(s) responsable(s) los costes totales de sustitución o reparación del equipo.

Las partes interesadas no deben:

- Intentar instalar software o aplicaciones no aprobados en dispositivos escolares.
- Descargar o acceder a software ilegal en dispositivos escolares.
- Descargar paquetes de software de la red escolar en soportes portátiles o dispositivos personales a no ser que se disponga del permiso correspondiente por parte del SLT y el Director de Tecnología de Europa.
- Intentar copiar o eliminar software de un dispositivo escolar.
- Intentar alterar la configuración del equipo de hardware o cualquier software que lo acompañe, a menos que se haga bajo la instrucción escrita del SLT y/o del Equipo Regional de TI.

7.4 La escuela proporciona recursos tecnológicos para acceder y almacenar datos y dispone de sistemas de filtrado para bloquear el acceso a material inadecuado, siempre que sea posible, para proteger el bienestar de las partes interesadas (más detalles en el Apéndice A-Declaración sobre filtrado web).

Las partes interesadas **no deben**:

- Eludir los sistemas de filtrado de sitios web y/o los sistemas de seguridad tecnológica (a través de la navegación "Tor", extensiones del navegador, VPNs o sistemas similares) mientras utilicen los dispositivos de la escuela dentro y/o fuera de las instalaciones.
- Acceder o intentar acceder a datos para los que no están autorizados.
- Interferir en el trabajo digital de otros usuarios
- Compartir información privada, sensible y/o confidencial a menos que

    - tengan autoridad para compartirla
    - el método para compartirla sea seguro y no utilice identificadores
    - el destinatario esté autorizado a recibir esa información
    - existan razones de salvaguarda (en cuyo caso sólo el equipo de Salvaguarda puede compartirla).

Es responsabilidad de los usuarios de la tecnología, cuando acceden a los datos, ser conscientes

de cualquier infracción de los derechos de propiedad intelectual, incluidos los derechos de autor, marcas registradas, patentes, diseños y derechos morales que puedan cometer.

7.5 La escuela se esfuerza por salvaguardar y, en la medida de lo posible, mitigar todos los riesgos de seguridad asociados a la tecnología y, en caso necesario, colaborará con el departamento regional de TI.

7.6 Las preocupaciones relativas a cualquiera de los siguientes puntos deben ser comunicadas al/a la Director/a o a un miembro del SLT que, según sea necesario, se pondrá en contacto con la Responsable Jefe Regional de Protección del Menor y/o con el Equipo Regional de TI tan pronto como sea posible en el mismo día:

- Acceso a material/contenido inapropiado en un dispositivo escolar o en la red escolar
- Uso indebido de la tecnología que haya causado daño o abuso a otra persona (o que pueda causarlo), de forma proporcional a cada caso.
- Preocupación por virus y otros programas maliciosos
- Correos electrónicos, enlaces y/o sitios web sospechosos o cualquier otra comunicación

7.7 Es responsabilidad de todos los usuarios de tecnología garantizar el **Bienestar** propio y de los demás tanto en dispositivos personales como escolares. Las partes interesadas **no deben**:

- Usar su propia tecnología o la de la escuela para intimidar a otros en línea (ciberacoso) o interrumpir el aprendizaje de los demás
- Utilizar su propia tecnología o la de la escuela para ponerse en contacto o relacionarse con personas que no conocen.
- Utilizar su propia tecnología o la de la escuela para crear, almacenar o compartir contenidos sexualizados y/o inapropiados/ilegales, incluyendo imágenes, audio, vídeo y/o texto.

Las partes interesadas deben:

- Informar de cualquier preocupación relacionada con el bienestar asociada al uso de la tecnología a un profesor, miembro del Equipo de Liderazgo Escolar o DSL/CPC a la primera oportunidad.

El personal nunca debe reenviar contenido inapropiado que haya recibido de un/a niño/a, padre, madre o miembro del personal a ningún otro niño/a, padre, madre o miembro del personal. Si reciben algo de esta naturaleza, deben notificarlo inmediatamente al DSL/CPC y al/a la Director/a, que pedirá consejo a la Responsable Regional de Protección del Menor. El personal no debe borrar el contenido hasta que se le indique.

7.8 Internet ofrece a los usuarios oportunidades sin precedentes para obtener información, participar en debates, colaborar y relacionarse con personas, organizaciones y grupos de todo el mundo con el fin de aumentar sus competencias, conocimientos, concienciación y capacidades

7.9 La escuela proporciona un acceso adecuado a **Internet y a las redes sociales** para apoyar

la educación y el funcionamiento de la escuela**.**

7.10 La escuela apoya activamente el acceso a la más amplia variedad de recursos de información disponibles, acompañado del desarrollo de las habilidades necesarias para filtrar, analizar, interpretar y evaluar la información encontrada. Las partes interesadas no deben:

- Utilizar un dispositivo escolar o la red escolar para visitar intencionadamente sitios de Internet que contengan contenidos obscenos, ilegales, que inciten al odio, abusivos, ofensivos, pornográficos, extremistas o inapropiados por cualquier otro motivo.
- Utilizar un dispositivo escolar o la red escolar para acceder a sitios web de juegos de azar.
- Conectarse (ya sea a título personal o profesional) con alumnos/as menores de diecinueve años en cualquier red social o a través de teléfonos móviles personales, o plataformas profesionales. En caso de recibir una solicitud de conexión, no deben responder (consulte el Código de Conducta).
- Hacer comentarios ofensivos o inapropiados, incluyendo desprestigiar el nombre y la reputación de la escuela, y/o sobre cualquier padre, madre, niño o niña asociado con la escuela, en cualquier foro/plataforma, tales como sitios de redes sociales (ya sea usando un dispositivo de la escuela o no) donde una conexión entre el usuario y la escuela pueda ser razonablemente hecha.

Las partes interesadas deben:

- Notificar a un miembro del SLT, DSL/CPC o del equipo de soporte de TI cualquier material/contenido inapropiado al que se haya accedido en un dispositivo escolar o en la red escolar para que se pueda investigar y bloquear el acceso de manera oportuna. En caso necesario, los centros escolares se pondrán en contacto con los colegas de apoyo regionales
- Reconocer y respetar la privacidad de las partes interesadas en las redes sociales.

8 Cognita Dispositivos Asignados: Acceso y Privacidad

8.1 Acceso a los dispositivos asignados y a los archivos digitales (contenido):

- Los dispositivos tecnológicos escolares asignados al personal y a los/las alumnos/as son para uso exclusivo del asignado
- Los dispositivos 1 a 1 de los/las alumnos/as pueden cargarse con una aplicación de gestión del aula que permita al profesorado controlar y ver la pantalla de los/las alumnos/as durante el periodo lectivo.
- Cognita se reserva el derecho a realizar inspecciones periódicas de los dispositivos para comprobar su estado físico y verificar que sólo tienen instalado software aprobado.
- Los dispositivos Cognita pueden estar equipados con aplicaciones de asistencia remota que permiten al personal de asistencia informática conectarse a los dispositivos para proporcionar asistencia remota; esta función sólo puede utilizarse con el permiso del responsable del dispositivo y el personal de asistencia informática se desconectará del dispositivo una vez finalizada la sesión.
- Cognita se reserva el derecho de acceder a un dispositivo asignado y supervisar su uso y contenido en las siguientes circunstancias especiales, entre otras:

- Para detectar y/o prevenir delitos
- Para permitir la protección de la seguridad del sistema (por ejemplo, virus, malware, piratería informática o cualquier otro riesgo).

- Para investigar posibles usos indebidos, abusos o actividades ilegales
- Investigar problemas de seguridad
- Supervisar el cumplimiento de las obligaciones laborales y legales.
- Garantizar la integridad de los dispositivos y sistemas informáticos de la escuela.

- Para acceder a un dispositivo asignado, se debe dar permiso por escrito de la siguiente manera:

    - Responsable de Recursos Humanos de Cognita para un dispositivo asignado a un miembro del personal
    - El/la Director/a del centro para un dispositivo asignado a un/a alumno/a

- Los datos contenidos en un dispositivo Cognita o a los que se acceda a través de un dispositivo Cognita se rigen por las políticas de privacidad de Cognita y del centro educativo.
- En las investigaciones de protección del menor, puede ser necesario acceder inmediatamente al dispositivo del/de la alumno/a o miembro del personal. Esto puede llevarse a cabo sin autorización por escrito cuando se sospeche que un/a alumno/a u otra persona pueda estar en riesgo de sufrir un daño. El acceso sólo puede ser realizado por un miembro del equipo de protección del menor, el/la Director/a, con el apoyo del departamento regional de TI cuando sea necesario. *Tenga en cuenta que el acceso no directo se realizará de forma rutinaria para llevar a cabo controles de supervisión (véase 4.4).

9 Fotografías e imágenes

9.1 El colegio se atiene a la legislación en materia de protección de datos, a saber, el Reglamento General de Protección de Datos de 2018 (modificado, ampliado o promulgado de nuevo cada cierto tiempo), así como a la normativa específica de cada país, y entiende que una imagen o un vídeo de un interesado se consideran datos personales sensibles. Solicita el consentimiento por escrito de las familias para publicar imágenes o vídeos con fines publicitarios o de marketing externos, como el sitio web de la escuela, y con fines internos, como un anuario o en un portal para padres. Los padres, tutores y alumnos mayores de 13 años (14 años en España) pueden retirar este permiso en cualquier momento a través del formulario "Uso de imágenes" y/o informando por escrito al Equipo de Administración del colegio.

9.2 El Código de Conducta del personal de Cognita establece que "Cognita no permite el uso de teléfonos móviles personales, dispositivos inteligentes y cámaras por parte del personal en presencia de alumnos".

9.3 Los dispositivos personales **nunca** deben utilizarse para tomar, almacenar o compartir imágenes de los/las alumnos/as.

9.4 El marco reglamentario de la etapa de educación infantil (Reino Unido) exige que todas las escuelas tengan una política clara sobre el uso de teléfonos y dispositivos móviles.

9.5 No se permite a las partes interesadas utilizar dispositivos de trabajo como teléfonos móviles, cámaras o grabadoras digitales para fotografiar o grabar a miembros del personal o a alumnos/as sin su permiso por escrito (en el caso de alumnos/as menores de 13 años, el permiso debe solicitarse por escrito a su familia). La escuela sólo podrá conceder el permiso en el caso de actuaciones/eventos organizados por la escuela (y se describirán claramente los límites).

9.6 Se ruega a los padres que sean considerados a la hora de tomar vídeos o fotografías en actos escolares (con permiso - véase el punto 9.5 anterior) y se les pide que no publiquen material de otros/as menores en ningún foro público sin el permiso de la familia correspondiente.

9.7 Es ilegal vender o distribuir grabaciones de actos sin permiso. 17.8. Toda familia que no desee que su hijo/a sea grabado/a en vídeo o fotografiado en actos escolares por otros asistentes deberá notificarlo al colegio con antelación y por escrito.

10 Utilización de equipos escolares para uso personal

10.1 En caso de que un miembro del personal decida utilizar el equipo y/o los sistemas informáticos para uso personal, se le informa de que lo hará bajo su propia responsabilidad y podría considerarse una infracción de esta política informática. Además, de acuerdo con el apartado 8 de esta Política, Cognita tiene derecho a acceder y supervisar el uso y el contenido de los equipos y la tecnología del centro, incluidas las comunicaciones personales que puedan haberse realizado a través de dichos medios del centro.

10.2 Solo podrán instalarse en un dispositivo de Cognita o utilizarse a través de un navegador programas y aplicaciones aprobados de acuerdo con el proceso de evaluación del impacto sobre la privacidad de los datos (DPIA) de Cognita. Para obtener más información sobre este proceso, haga clic aquí. Y aquí se encuentra una lista de software y aplicaciones aprobados (así como no aprobados y pendientes). Para más información sobre DPIA, consulte la sección 14 de esta política.

10.3 Los dispositivos y redes de la escuela no deben utilizarse para llevar a cabo ninguna actividad ilegal.

10.4 El personal no debe realizar ninguna transacción privada o financiera en los equipos compartidos, ya que esto conlleva el riesgo de una violación de datos.

11 Uso de equipos personales en la Escuela

11.1 Los dispositivos personales no deben conectarse a la red escolar, salvo a la red Wi-Fi para invitados y siempre que se tenga el consentimiento de la dirección del centro.

11.2 No deben utilizarse dispositivos personales en presencia de niños (véanse las secciones 9.2 y 9.3).

12 Procedimiento para notificar preocupaciones e incidentes

12.1 Las partes interesadas pueden tener preocupaciones con respecto a lo siguiente, en relación con la tecnología:

- Dispositivo/entorno inseguro y/o inapropiado
- acceso a material/contenido inadecuado
- amenaza de virus/malware u otra actividad maliciosa, incluida la piratería informática

- pérdida, daños o robo*.

*Cualquier caso de robo debe notificarse a la policía y se debe obtener un número de referencia del delito, que debe compartirse con un miembro del Equipo de Liderazgo y con el Servicio Regional de Informática.

Todos los problemas e incidentes deberán notificarse al Servicio de Atención al Cliente de Cognita: servicedesk@cognita.com o a través del Reino Unido: +44 3301244417; España +34936296806; Italia: +39055093073.

12.2 Deberán tomarse las siguientes medidas ante tales preocupaciones o incidentes:

- Detener el problema y/o retirar la tecnología afectada (a menos que hacerlo pudiera poner en peligro cualquier investigación interna o de una agencia externa, por ejemplo, la Policía).
- Evitar que el incidente se haga público
- Informar del incidente o de la preocupación a un miembro del personal docente, al/a la Director/a del centro, al DSL/CPC o al equipo de soporte informático, según proceda. Si la situación es compleja y grave, el/la Director/a deberá informar a la Responsable Regional de Protección del Menor y/o al Responsable Europeo de TI.
- Registrar la naturaleza del incidente y las personas implicadas utilizando los formularios adecuados en el momento y la forma indicados.
- Conservar las pruebas para permitir cualquier investigación, si fuera necesario

12.3 El personal **no debe** llevar a cabo ninguna investigación hasta que haya sido autorizado para ello por el/la Director/a, la Responsable Regional de Protección del Menor y/o el Responsable Europeo de TI.

12.4 El Director/DSL/CPC u otro miembro del personal designado deberá cumplimentar el Formulario de Incidente Grave (SIRF), siguiendo las instrucciones de la Responsable de Salud y Seguridad/Responsable Regional de Protección del Menor, después de cualquier investigación.

12.5 El personal debe informar a un miembro del Equipo de Liderazgo o al DSL/CPC cuando:

- sean testigos o sospechen que las partes interesadas han accedido a material/contenido inadecuado
- sean testigos o sospechen que se están utilizando los chats de equipo para interrumpir el aprendizaje o molestar al personal o a los/las alumnos/as.
- pueden acceder a material/contenido inadecuado
- están enseñando temas que podrían crear una actividad inusual en los registros de filtrado
- hay fallos en el software y/o abuso del sistema
- se perciben restricciones poco razonables que afectan a la enseñanza y el aprendizaje o a las tareas administrativas
- observan abreviaturas o faltas de ortografía que permiten el acceso a material

restringido

12.6 El acceso a material inadecuado y las preocupaciones relativas a virus y otros programas maliciosos en un dispositivo escolar o en la red escolar deben comunicarse a un miembro del personal docente, a un miembro del Equipo de Liderazgo Escolar o al Equipo de Apoyo Informático lo antes posible en el mismo día.

12.7 La pérdida, el daño o el robo de tecnología escolar debe comunicarse a un miembro del personal docente, a un miembro del equipo de dirección del centro o al equipo de soporte informático lo antes posible en el mismo día; el robo también debe comunicarse a la policía y debe obtenerse una referencia del delito (véase más arriba).

12.8 Los/las alumnos/as deben responsabilizarse del uso que hacen de los equipos informáticos tanto en el colegio como en casa; en caso de que las familias tengan dudas o se percaten de algún problema, recomendamos encarecidamente que se pongan en contacto con el colegio lo antes posible para que podamos ofrecerles asesoramiento y apoyo.

12.9 La escuela tiene la obligación de informar a las autoridades (servicios sociales) o a la policía de los problemas graves de protección relacionados con las partes interesadas, de acuerdo con los requisitos legales (véase la política de protección).

13 Eliminación del acceso a la red, cuentas y dispositivos

13.1. Se podrá retirar el acceso a la red, la(s) cuenta(s) o el dispositivo a toda persona que infrinja la Política de TI y podrá ser objeto de medidas disciplinarias adicionales.

13.2 El centro escolar y el Equipo Regional de Informática se reservan el derecho de retirar el acceso a la red en cualquier momento.

13.3. La escuela podrá informar a la policía o a cualquier otro organismo encargado de hacer cumplir la ley en caso de que se produzca cualquier uso que pueda dar lugar a un procedimiento penal.

13.4. La escuela asume seriamente sus responsabilidades en relación con la seguridad digital y el uso de la tecnología por parte de los interesados y es consciente de la importancia de supervisar, evaluar y revisar periódicamente sus políticas y procedimientos.

14 Evaluación del impacto sobre la privacidad de los datos (DPIA)

2.1. Cognita realiza una DPIA de las aplicaciones, sitios web, software y servicios, colectivamente «terceros», en los que se recopilan datos personales. Con ello se pretende garantizar que se puede confiar al tercero nuestra información, en particular la relativa a menores. Para obtener más información sobre este proceso, haga clic aquí.

Las partes interesadas deben:

- utilizar únicamente terceros autorizados (consulte la lista aquí)
- limitar la cantidad de datos personales revelados al tercero (sólo compartir la información necesaria para el funcionamiento del producto/servicio)
- cumplir las condiciones de uso del tercero. Esto suele incluir (aunque no siempre) lo siguiente

- una restricción de edad (en el caso de aplicaciones, sitios web y programas informáticos dirigidos a estudiantes, suele ser, aunque no siempre, 13 años)
- consentimiento de una persona adulta apropiado (por ejemplo, personal docente, familiar) para que el/la niño/a utilice el producto/servicio de terceros
- el requisito de que una persona adulta adecuada (por ejemplo, personal docente o familiar) cree una cuenta para el/la niño/a.

Las partes interesadas no deben

- participar en foros en línea/públicos que puedan aparecer en una aplicación y/o sitio web
- relacionarse con usuarios desconocidos a través de una aplicación y/o sitio web
- utilizar terceros no aprobados y/o pendientes de aprobación a menos que se autorice por escrito

15 Inteligencia Artificial (IA)

15.1 Consulte la **Declaración de Cognita sobre la Inteligencia Artificial en la Educación**.** **A partir de junio de 2024, esta declaración se está redactando de nuevo. La política regional de TI se actualizará después de la nueva redacción y los lectores serán dirigidos a la declaración a través de un enlace**.**

16 Traiga su propio dispositivo (BYOD por sus siglas en inglés)

Cognita comprende la importancia de la tecnología y del acceso online para apoyar los objetivos de enseñanza y aprendizaje. Sin embargo, la necesidad de acceder a contenidos online debe equilibrarse con la seguridad online de nuestras partes interesadas, especialmente de nuestros/as alumnos/as.

BYOD es la práctica que permite a los individuos traer sus propios dispositivos tecnológicos (personales) a las instalaciones. A partir de junio de 2024, la postura BYOD de Cognita difiere entre el personal y los/las alumnos/as:

16.1 Se permite al personal traer un dispositivo personal a las instalaciones, pero no debe:

- utilizar dicho dispositivo en presencia de alumnos
- conectar dicho dispositivo a una red escolar, sólo a la red WIFI de invitados
- no realizar tareas relacionadas con el trabajo en su dispositivo personal

16.2 Los estudiantes no deben utilizar un dispositivo personal en el centro a menos que cuenten con la autorización por escrito de un miembro del SLT y/o del departamento regional de TI. Los/las alumnos/as deben tener una razón excepcional para no utilizar su dispositivo suministrado por la escuela.

16.3 Durante el curso académico 2024-25, Cognita explorará el BYOD en el contexto de los/las alumnos/as e iniciará una prueba de BYOD en algunos de nuestros centros. Dicha prueba determinará la futura postura de Cognita en términos de BYOD para los alumnos.

17 Comunicación en línea y mensajes instantáneos

17.1 Para evitar que los/las alumnos/as participen en comunicaciones perjudiciales o inapropiadas, Cognita ha establecido restricciones en determinados canales de comunicación. Estas restricciones están establecidas por defecto, pero pueden modificarse para centros y/o alumnos/as concretos previa solicitud del/de la Director/a del centro y aprobación del Responsable Regional de Informática. En la tabla siguiente se indica lo que está o no está disponible por defecto para los/las alumnos/as:

Email			MS Teams	
Enviar fuera de la organización*	**Recibir de fuera de la organización**	**Enviar/recibir entre colegios Cognita**	**Función de chat**	**Publicar un post en un canal de Teams (donde son miembros)****
✓	✗	✗	✗	✓

*Para aclarar – los/las alumnos/as que envían correos electrónicos externos deben tener permiso por escrito SLT e incluir un miembro del personal docente en copia de su correo electrónico saliente.

**Para aclarar, los/as alumnos/as pueden, y deben, solo dejar mensajes de Teams en espacios creados y gestionados por el personal docente. Los/las alumnos/as no deben crear equipos en MS Teams.

18 Anexo A- Declaración sobre Filtrado de Web

La declaración que figura a continuación ofrece información detallada sobre las medidas adoptadas para filtrar y controlar el uso de Internet en los centros escolares Cognita.

Todo el uso de Internet en los centros se filtra y supervisa. Todo el tráfico de la red se dirige a través de DNS a Cleanbrowsing, una solución de filtrado SafeSearch basada en la nube. Cleanbrowsing proporciona medidas de protección que bloquean o filtran el acceso a Internet a imágenes que son: (a) obscenas; (b) pornografía infantil; o (c) perjudiciales para menores. Por defecto, Google Chrome y Microsoft Edge están configurados en Modo Seguro. Se bloquean los dominios maliciosos y de phishing. El filtro de seguridad bloquea el acceso a dominios de phishing, spam, malware y maliciosos. La base de datos de dominios maliciosos se actualiza cada hora y está considerada como una de las mejores del sector.

Todo el tráfico de red está filtrado desde el sitio por los cortafuegos Smoothwall, Watchguard o Fortinet. Se aplican políticas específicas de filtrado web a distintos grupos por centro (por ejemplo, personal, alumnos/as de Bachillerato, de Primaria o Secundaria). Smoothwall analiza el tráfico en función de un conjunto de políticas configuradas para el centro y permite o bloquea el acceso a los sitios web en función de su categorización y contenido.

Todos los dispositivos 1 a 1 de los/las alumnos/as tienen instalado un agente de filtrado web Lightspeed que utiliza IA avanzada para bloquear automáticamente millones de sitios, imágenes y vídeos inapropiados y dañinos.

Tanto Smoothwall, Fortinet, Watchguard como Lightspeed registran las actividades para su análisis, investigación y elaboración de informes. El análisis del tráfico y del uso de Internet se evalúa periódicamente para actualizar las reglas de filtrado.

Más información sobre las respuestas del proveedor de supervisión de Lightspeed, que pone de relieve hasta qué punto nuestra herramienta de filtrado bloquea los contenidos nocivos e inadecuados, sin afectar injustificadamente a la enseñanza y el aprendizaje: https://www.lightspeedsystems.com/media-release/lightspeed-systems-gains-uk-safer-internet-centre-accreditation/

La Responsable Regional de Protección del Menor está disponible para ayudar con cualquier problema relacionado con la salvaguardia que requiera una intensificación.

Los miembros del equipo regional de TI de Cognita están a su disposición para cualquier asunto que requiera una ampliación.

Contactos principales:

- Jefe de TI de Cognita - Europa y EEUU
- Responsable regional de protección del menor
- Jefe de seguridad cibernética del grupo

Anexo B - Formulario de consentimiento de uso del iPad/portátil 1 a 1 del alumno

ACUERDO DE USO DEL iPAD/LAPTOP 1-a-1 DEL ALUMNO

- A partir de ahora, tu nuevo iPad/portátil formará parte de tu experiencia de aprendizaje en el colegio. Trátalo con cuidado y utilízalo para colaborar con tus profesores/as y compañeros/as de clase de una forma útil que contribuya a tu aprendizaje. A continuación, te ofrecemos unas sencillas pautas que te ayudarán a mantenerte seguro y responsable cuando utilices tu dispositivo 1 a 1. Léelas y comprométete firmemente a cuidar de tu dispositivo y a mantenerte a ti y a tus compañeros/as seguros/as mientras trabajas en el entorno virtual.

ASEGÚRATE

- Visita sólo sitios web que apoyen los objetivos de aprendizaje asignados por tus profesores/as.
- Habla con tus compañeros/as a través de tu dispositivo para colaborar en las tareas de aprendizaje y recuerda que siempre debes interactuar con los demás como si la conversación fuera cara a cara. Sé amable y respetuoso/a en todo momento.
- Tu dispositivo tiene todas las aplicaciones y el software necesarios para que aprendas y trabajes con eficacia. No instales ninguna aplicación ni cambies ninguna configuración a menos que tu profesor/a te lo haya pedido.

SE RESPONSABLE

- Mantén tu iPad/portátil a salvo cuando te desplaces.
- Guarda tu iPad/portátil bajo llave cuando no lo lleves contigo o guárdalo en un lugar seguro.
- Maneja tu iPad/portátil con cuidado manteniéndolo alejado de alimentos y líquidos.
- Notifica cualquier daño o problema a tu profesor/a.
- No utilices tinta permanente, adhesivos ni cualquier otra sustancia abrasiva que pueda dañar estética o físicamente el dispositivo

Me comprometo a cuidar muy bien de mi iPad/portátil manteniéndolo en un lugar seguro, y a ser siempre responsable y respetuoso/a con los/las demás en mis palabras y acciones cuando lo utilice.

Nombre:

Fecha:

19 Anexo C – Políticas Relacionadas

Europa & EUA

- Safeguarding and Child Protection Policy
- Preventing Radicalisation Policy
- Behaviour Policy
- Code of Conduct Policy
- Personal and Professional Boundaries Policy
- Student Charter
- Data Protection Policy

Group IT

- Group Policy - Software (Applications)
- Cognita_Password_Policy.pdf
- Personal and Professional Boundaries Policy
- Cognita_Cyber_Security_Policy.pdf
- Cognita Safeguarding Systems_Cyber Security Policy

20 Anexo D – Recursos Online

Department for Education (DfE)

- Keeping Children Safe in Education (KCSIE)
- Meeting digital and technology standards in schools and colleges
- Data Protection in Schools
- The Prevent Duty

Information Commissioner's Office (ICO)

- Data Protection Impact Assessment

London Grid for Learning (LGfL)

- Online Safety Audit

Southwest Grid for Learning (SWGfL)

- Online Safety Self-Review Tool for Schools

National Cyber Security Centre

- Cyber security training for school staff

Other

- UK Safer Internet Centre
- Digital Resilience

Propiedad y Consultoría	
Document sponsor/approver	Head of IT – Europe & United States
Document author	Head of IT – Europe & United States
Consultation with	Europe Digital Learning Advisors
	Group Cyber Security
	Europe IT POD Leads
	Regional Safeguarding Lead (Europe and North America)
Audiencia	
Audiencia	Regional Employees
	Regional Students and Parents
	Suppliers
	Visitors
	Contractors
Aplicación del documento	
The policy is related to this jurisdiction	All Cognita Europe & United States Schools and Offices
Control de versión	
Review cycle	Annual
Effective from	September 2024
Next review date	September 2025
Version	1.0 ISSUED