COGNITA

Europa

Política de TI

Septiembre 2026

41–42 Eastcastle Street, London W1W 8DY, UK. T +44 (0)20 7636 8444. www.cognita.com
Cognita Schools Limited No 02313425. Registered Office: Seebeck House, One Seebeck Place, Knowlhill, Milton Keynes MK5 8F

Contenido

1	Introducción	3
2	Objetivo de la política	3
3	Ámbito de aplicación de la política	3
4	Roles y responsabilidades	4
5	Uso seguro de la tecnología	5
6	Derecho de uso de redes y dispositivos educativos/corporativos	7
7	Uso apropiado de la tecnología para garantizar la seguridad digital	8
8	Dispositivos propiedad de Cognita: Acceso & Privacidad	11
9	Fotografías e Imágenes	12
10	Uso de dispositivos educativos/corporativos para uso personal	13
11	Uso de dispositivos personales en el colegio	13
12	Procedimiento para reportar preocupaciones e incidentes	13
13	Eliminación de acceso a la red, cuentas y dispositivos	15
14	Data Privacy Impact Assessment (DPIA)	15
15	Inteligencia Artificial (IA)	16
16	Bring Your Own Device (BYOD)	16
17	Comunicación online y mensajería instantánea	17
18	Monitorización de la actividad online del alumnado	19
19	Uso de Drones	20
19	Uso de dispositivos inteligentes y seguimiento de usuarios	20
20	Anexo A- Filtrado Web	18
21	Anexo C – Políticas relacionadas	20
22	Anexo D – Recursos online relacionados	20

1 Introducción

El uso de 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 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 que las familias participen y ayuden al centro a salvaguardar el bienestar de los/las alumnos/as y fomentar un 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 puesta a disposición de las partes interesadas, tanto en los centros escolares como en las oficinas regionales (dentro o fuera de las instalaciones).

2.2 Definir el uso aceptable e inaceptable de la tecnología en 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 a 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 o desconocidas) fuera de la escuela.
- Conducta inapropiada cuando se use la tecnología
- Ciberacoso y/o abuso online
- Copia y compartición de datos personales
- Riesgos relacionados con el comercio digital; 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 de seguridad y para mantenerse a salvo.

3 Aplicación de la política

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

3.2 Los colegios adoptarán un enfoque amplio 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 del centro , WIFI y acceso a Internet
- Hardware y dispositivos digitales, incluyendo a los dispositivos "inteligentes" e IOT
- Software
- 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)

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

4 Roles y responsabilidades

El responsable de esta política es el Head of IT de Cognita Europa y Norteamérica, quien garantizará que la tecnología se implante y supervise de acuerdo con esta política, así como cumpliendo con otras políticas pertinentes.

4.1. Los/las Directores/as Generales de cada grupo de colegios y los/las Directores/as de los centros educativos son responsables de la publicación de esta política y de su aplicación y supervisión continua 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 de ciberseguridad , en cumplimiento con la política global de Cognita, incluyendo el proceso de filtrado y supervisión de contenidos online.

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 otros miembros del equipo 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 seguridad, bienestar y salvaguarda 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).

- Comunicar cualquier inquietud relacionada con los sistemas de monitoreo y control de contenidos y/o los resultados que estos entreguen relativos a alumnos/as a la persona Responsable Regional de Protección de Menores (quien, en caso necesario, remitirá la cuestión al Responsable IT de Europa y Estados Unidos si se trata de un problema relacionado con la tecnología).
- Asegurarse de que el personal de los centros haya recibido formación relativa a 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, así como de los potenciales riesgos de la actividad online.

5 Uso seguro de la tecnología

5.1 El colegio está comprometido con el uso seguro y útil de la tecnología para la enseñanza, el aprendizaje y la administración del centro

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 El colegio 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 proteger a las partes interesadas.

5.5 Las herramientas de filtrado y supervisión se revisan anualmente de forma centralizada para garantizar que sus disposiciones actuales satisfagan 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 Directivos 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.

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, incluyendo a 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 contenidos para adultos, radicalización, violencia, odio y racismo, actividades delictivas y terrorismo*.

5.12. El centro escolar puede solicitar cambios a medida para bloquear/desbloquear sitios para su centro, y deberá solicitarlo a través del Service Desk de Cognita o del Responsable de TI del centro.

5.13. El colegio no debe usar sistemas de filtrado alternativos. El equipo regional de TI se encarga de realizar periódicamente todas las tareas de filtrado, inclusión en listas de dominios aprobados o denegados y pruebas, y es responsable de garantizar que los sistemas de filtrado web del colegio sean eficaces.

5.14. Es responsabilidad de cada colegio educar a su alumnado acerca de la importancia del uso seguro y responsable de la tecnología para ayudarles a protegerse a sí mismos y a los demás mientras estén online. Los equipos de TI y de aprendizaje digital apoyan esto a través de diversos recursos, políticas (incluida ésta) y formaciones.

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 y efectivo de la tecnología por parte de los/las alumnos/as y fomentar su aprendizaje y destrezas digitales.

5.16. Cualquier inquietud 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.

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 IT de Europa y Estados Unidos (para asuntos tecnológicos) y a la Responsable Regional de Protección de Menores (para asuntos de protección de menores), quienes contactarán 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 tienen a su disposición los siguientes recursos 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 cumplir las normas de ciberseguridad establecidas por las autoridades locales y nacionales.

Para ayudar a los centros a cumplir con estas obligaciones, 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 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 las necesidades de protección de cada centro.

Aunque no existe en la UE un equivalente tan específico y prescriptivo como la norma del Ministerio de Educación del Reino Unido (DfE) sobre filtrado y supervisión, sí existen marcos y directrices a nivel europeo, tales como:

Digital learning and ICT in education | Shaping Europe's digital future

Home - Better Internet for Kids

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 sus cuentas personales, 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 ningún otro servicio 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 serán gestionado por el profesorado.

6.4 Toda la tecnología del centro educativo seguirá siendo propiedad de Cognita. El centro podrá solicitar 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. 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 profesorado o personal no educativo no deben utilizarse para tareas relacionadas con el trabajo dentro del colegio, y nunca deben utilizarse en presencia de alumnos/as.

6.7 Se prohíbe cualquier intento de acceso o utilización de 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 "Formulario de solicitud de acceso al buzón y a los archivos" al Service Desk de Cognita.

6.8 Los dispositivos designados al personal y alumnos son entregados para impartir la enseñanza, el aprendizaje y la administración del centro:

- Los/las alumnos/as a los que se ha asignado un dispositivo 1-to-1 deberán firmar el Acuerdo de Uso del dispositivo (enlace en el Apéndice)
- Los/las alumnos/as a los que se ha asignado un dispositivo 1-to-1 pueden utilizarlo en las clases bajo las directrices del profesorado
- Las familias son responsables del coste de la reparación o sustitución por otro equipo del mismo fabricante, modelo y características de un dispositivo asignado a un alumno/a (según las instrucciones de la escuela), si se daña / pierde intencionadamente o bien por negligencia.
- El personal y los/las alumnos/as de Cognita son responsables de la seguridad del dispositivo que les ha sido asignado cuando estén fuera de las instalaciones del centro.
- Los dispositivos y los periféricos proporcionados por la escuela o Cognita 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 que se entreguen al personal que estén dañados y/o defectuosos se reparan o sustituyen por otros de características similares, y los costes son cubiertos de forma centralizada o por la escuela.

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 esta no esté en uso.
- Utilizar aplicaciones de mensajería móvil para comunicarse con las familias, así como en el caso del personal de los centros, tampoco debe contactar con los/las alumnos/as.
- Enviar mensajes y/o correos electrónicos desde cuentas del colegio que se hagan pasar por un tercero y que no es quien 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 del colegio.

- Se espera que los usuarios de los dispositivos en propiedad del centro tengan cuidado de los mismos de forma responsable.
- Los dispositivos tecnológicos del centro no deben salir 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.

- Los dispositivos asignados al personal y al alumnado son responsabilidad de la persona a quien le han sido asignados.

- Las partes interesadas **no deben** dejar desatendidos los equipos tecnológicos portátiles, incluidos los dispositivos proporcionados por el colegio , a menos que dichos equipos no estén en 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 Soporte TI en el mismo día en que se produzca la pérdida o daño.
- El robo de un dispositivo asignado a un miembro 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 Soporte TI en el mismo día, incluyendo el número de referencia del delito de la Policía. En caso de que el robo se produzca dentro del 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 o páginas web ilegales en dispositivos escolares.
- Descargar software disponible en la red del centro a soportes portátiles de almacenamiento o a dispositivos personales, a menos 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 hardware o software que acompaña al equipo.

7.4 El colegio proporciona **recursos tecnológicos** para acceder y almacenar datos, así como dispone de sistemas de filtrado para bloquear el acceso a material inadecuado, siempre que esto 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 del colegio 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
    - la persona que recibe la información está autorizada a hacerlo
    - hay razones comerciales legítimas
    - existen razones legítimas de salvaguarda

Al acceder a los datos, es responsabilidad de los usuarios 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 El colegio se esfuerza por salvaguardar y, en la medida de lo posible, mitigar todos los **riesgos de seguridad** asociados al uso de 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 quién según sea necesario, se pondrá en contacto con la Responsable 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 del colegio
- Uso indebido de la tecnología que haya causado daño o abuso a otra persona (o que pueda causarlo), incluyendo, pero no limitado a:
    - Ciberacoso
    - *Upskirting*
    - Creación y/o intercambio de imágenes o videos íntimos generados por usuarios, incluyendo los generados con IA, como, por ejemplo, *deepfakes*
    - Creación y/o intercambio de material generado por IA que es, o podría ser, considerado abusivo
    - Creación y/o intercambio de desnudos o semi desnudos
    - Chantaje
    - Grooming o extorsión sexual
- 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 del colegio para intimidar a otros en línea (ciberacoso) o interrumpir el aprendizaje de los demás
- Utilizar su propia tecnología o la del colegio para ponerse en contacto o relacionarse con personas que no conocen.
- Utilizar su propia tecnología o la del colegio 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 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 colegio proporciona un acceso adecuado a Internet y a las redes sociales para apoyar la educación y el funcionamiento de la colegio.

7.10 La colegio 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. No obstante, las partes interesadas no deben:

- Utilizar un dispositivo del colegio o la red del colegio 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 del colegio o la red del colegio para acceder a sitios web de juegos de azar.
  •Comunicarse o conectar con alumnos/as a través de cuentas personales en redes sociales, servicios de mensajería personal o dispositivos móviles personales. Esto se aplica a todos los/las menores de 18 años, de acuerdo con las directrices de protección infantil. En caso de recibir una solicitud de conexión de un/a alumno/a (ya sea actual o antiguo/a), no deben responder (consulte el Código de Conducta).
- Hacer comentarios/imágenes ofensivos o inapropiados, incluyendo desprestigiar el nombre y la reputación de la colegio, y/o sobre cualquier padre, madre, niño o niña asociado con el colegio, en cualquier foro/plataforma, tales como sitios de redes sociales (ya sea usando un dispositivo del colegio o no) donde una conexión entre el usuario y el colegio 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 del colegio o en la red del colegio para que se pueda investigar y bloquear el acceso de manera oportuna. En caso necesario, los colegios se pondrán en contacto con los colegas de apoyo regionales
- Reconocer y respetar la privacidad de las partes interesadas en las redes sociales y sitios web.

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 1:1 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 solo 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 solo 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 del colegio.

- 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 solo 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, así como a la normativa específica de cada país, y entiende que una imagen o un vídeo de un interesado se considera datos personales. Solicita el consentimiento por escrito de las familias para publicar imágenes o vídeos con fines no esenciales, (fines publicitarios o de marketing, como el sitio web de la colegio), y con fines internos esenciales como CCTV. Las familias y alumnado de una cierta edad según legislación local 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 y la Política de Protección Integral de Menores establece que "Cognita no permite el uso de cualquier dispositivo personal capaz de capturar o compartir imágenes/vídeos y/o datos en la presencia de alumnado, ya sea dentro o fuera del recinto del colegio. Incluye teléfonos móviles, tabletas, de teléfonos dispositivos inteligentes como teléfonos, relojes, gafas, joyas, y otros *hearables* y *wearables.*

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 todos los colegios en el Reino Unido tengan una política clara sobre el uso de teléfonos y dispositivos móviles. Véase la Política de Comportamiento de Cognita.

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 una edad especificada en la legislación local, el permiso debe solicitarse por escrito a su familia. La colegio solo podrá conceder el permiso en el caso de actuaciones/eventos organizados por la colegio (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 del colegio para uso personal

10.1 Los dispositivos y sistemas informáticos del centro se facilitan para el trabajo escolar y con fines profesionales. No obstante, reconocemos que el personal puede utilizar ocasionalmente los dispositivos de trabajo para fines personales. En caso de que un miembro del personal decida utilizar el equipo y/o los sistemas informáticos para fines personales, se le informa de que lo hará bajo su exclusiva responsabilidad. Dependiendo del uso que se le dé, podría considerarse un incumplimiento de la presente Política de TI. Por ejemplo, navegar por sitios web fuera del horario laboral y en ausencia de los alumnos (p. ej., durante los descansos, la hora de comer, etc.) se considera generalmente aceptable, siempre que el sitio web sea seguro y adecuado. Tenga en cuenta que, de conformidad con la sección 8 de esta Política, Cognita tiene derecho a acceder y supervisar el uso y el contenido de los equipos y la tecnología del colegio, incluidas las comunicaciones personales que puedan haberse realizado a través de dichos medios del colegio.

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 colegio 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 Colegio

11.1 Los dispositivos personales no deben conectarse a la red del colegio, salvo a la red Wi-Fi para invitados

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

- No se deben utilizar dispositivos personales con fines escolares o laborales, ya que ello conlleva numerosos riesgos de seguridad, entre los que se incluyen, entre otros:
- controles de seguridad más débiles, debido a que los servicios de seguridad de los dispositivos no cumplen con la normativa
- software obsoleto, lo que deja vulnerabilidades sin parchear y pone en riesgo al usuario
- fuga o exposición de datos: los archivos de trabajo confidenciales podrían sincronizarse accidentalmente con servicios en la nube personales
- Las preocupaciones desde el punto de vista de la privacidad de los datos incluyen, entre otras:
- Mezcla de datos personales y corporativos: lo que dificulta el control del destino de la información de la empresa
- Riesgo de pérdida o robo del dispositivo: si se pierde un dispositivo personal con datos de la empresa, podrían quedar expuestos tanto los datos personales como los de la empresa.
- Uso familiar o compartido: si otras personas utilizan el dispositivo personal del interesado, podrían acceder involuntariamente a material de trabajo confidencial

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:

Reino Unido	servicedesk@cognita.com	+44 3301244417
España	servicedesk@cognita.com	+34936296806;
Italia	servicedesk@cognita.com	+39055093073.

12.1 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 de Europa y Estados Unidos de IT.
- 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

12.2 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 de Europa y Estados Unidos de IT.

12.3 El/la directora/a o 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.

12.4 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

12.5 El acceso a material inadecuado y las preocupaciones relativas a virus y otros programas maliciosos en un dispositivo del colegio o en la red del colegio 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.

12.6 La pérdida, el daño o el robo de tecnología del colegio 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).

12.7 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.

12.8 La colegio 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 colegio y el Equipo Regional de Informática se reservan el derecho de retirar el acceso a la red en cualquier momento.

13.3 La colegio 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 colegio 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 Recuperación de archivos personales de antiguos empleados

14.1. Cognita desaconseja encarecidamente el almacenamiento de archivos personales en dispositivos de trabajo* (consulte la sección 10, «Uso del equipamiento del centro educativo con fines personales», de la presente política). No obstante, reconocemos que esto puede ocurrir ocasionalmente. Por ello, es responsabilidad de los/las empleados/as asegurarse de que todos los archivos personales se eliminen de los sistemas de la empresa antes de su salida.

*Tenga en cuenta que todos los archivos almacenados en dispositivos y/o sistemas de trabajo se consideran propiedad de la empresa.

14.2. Si un/a antiguo/a empleado/a no puede recuperar sus archivos personales y posteriormente necesita acceder a ellos, la solicitud se tratará caso por caso y a la entera discreción de los departamentos de RR. HH. y TI de Cognita. Tenga en cuenta que ninguno de los dos departamentos está obligado a restablecer el acceso a la cuenta. Para la recuperación de archivos se seguirán los siguientes pasos:

- **Ubicación de los archivos**: el/la antiguo/a empleado/a deberá proporcionar instrucciones claras a los departamentos de RR. HH. y TI sobre la ubicación de los archivos.
- **Recopilación de datos**: las solicitudes deben ser específicas y concretas. No se aceptarán solicitudes generales o vagas (por ejemplo, «Todo lo personal de mi buzón de correo / OneDrive»).
- **Revisión del contenido**: se revisarán los archivos para garantizar que se excluyan los materiales empresariales, confidenciales u objeto de controversia. Se requerirá el consentimiento por escrito del/de la antiguo/a empleado/a antes de cualquier entrega.

14.3. En determinadas circunstancias, Cognita puede verse legalmente obligada a denegar o censurar el contenido de los archivos. Esto incluye los siguientes casos:

- El/la empleado/a fue despedido/a por una falta grave relacionada con las tecnologías de la información o los datos
- Los archivos no pueden separarse claramente de los datos relacionados con la actividad empresarial
- La solicitud de acceso es desproporcionada
- Existe un litigio o una investigación en curso
- La solicitud es imprecisa o excesiva

En caso de que se faciliten los archivos, se hará de forma segura y controlada.

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

15.1 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 (solo 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

16 Sitios web y filtrado

Para proteger a nuestras partes interesadas, Cognita utiliza un sistema de filtrado web en todos los dispositivos conectados a la red, lo que contribuye a garantizar que el uso de Internet se ajuste a nuestras normas de seguridad, cumplimiento normativo y productividad. El sistema de filtrado web está diseñado para:

- **Mejorar la seguridad** bloqueando el acceso a sitios web maliciosos o de alto riesgo que puedan considerarse inapropiados y/o que contengan virus, intentos de phishing o contenido perjudicial

- **Proteger la información** confidencial impidiendo el acceso a sitios o servicios que puedan dar lugar a fugas de datos

- **Facilitar el cumplimiento** de los requisitos legales, normativos y contractuales relativos al uso de Internet y a la protección de datos

Se anima a los empleados a utilizar Internet de forma responsable y de acuerdo con las políticas de la empresa.

Las solicitudes para desbloquear sitios web, incluidos aquellos creados por profesores de (Cognita) o por creadores independientes, son cada vez más frecuentes. Aunque permitir a los alumnos el acceso a dichos sitios web puede resultar valioso para el aprendizaje, también conlleva riesgos, entre los que se incluyen, entre otros:

- **enlaces inapropiados**: los enlaces externos o los contenidos multimedia incrustados podrían llevar a los alumnos a sitios inadecuados o inseguros.
- **interacción no moderada y/o en redes sociales**: si el sitio cuenta con foros, secciones de comentarios o funciones de chat, podría dar pie al acoso, al hostigamiento o a interacciones inapropiadas.
- **malware o vulnerabilidades**: si el sitio no se mantiene con regularidad, podría ser objeto de un ataque informático y difundir contenido malicioso.

Por lo tanto, el departamento regional de TI no aprobará las solicitudes de páginas web en las que se detecte alguna de las situaciones mencionadas anteriormente en dicha página web.

17 Inteligencia Artificial (IA)

17.1 Consulte la Política **de Cognita sobre la Inteligencia Artificial**

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

18.1 El personal puede traer un dispositivo personal al centro, pero no debe:

- utilizar dicho dispositivo en presencia de los alumnos
- conectar dicho dispositivo a la red del centro, sino únicamente a la red Wi-Fi para invitados
- realizar tareas relacionadas con el trabajo en su dispositivo personal,

18.2 Los alumnos no deben utilizar dispositivos personales en las instalaciones a menos que cuenten con una autorización por escrito de un miembro del equipo directivo (SLT) y/o del departamento regional de TI. Los alumnos deben tener una razón excepcional para no utilizar el dispositivo proporcionado por el centro educativo.

19 Comunicación en línea y mensajes instantáneos

19.1 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		
Envíos externos	**Recepción externa**	**Enviar/recibir entre colegios Cognita**
No disponible	Parcialmente disponible	Disponible
Correos electrónicos salientes, es decir, aquellos en los que el alumnado desee comunicarse con personas externas: *1. deben contar con el permiso por escrito del equipo directivo (SLT) y del equipo regional de TI, mediante una solicitud enviada al servicio de asistencia técnica de Cognita; y* *2. deben incluir a un docente en copia en el correo electrónico saliente.*	*-Los correos electrónicos entrantes (dirigidos a alumnado) están bloqueados por defecto. No obstante, pueden desbloquearse cuando el remitente forme parte de un tercero autorizado (como un proveedor de aplicaciones o software que haya superado el proceso de DPIA de Cognita).* *Es posible que dichos terceros tengan que enviar un correo electrónico al/a la alumno/a para verificar su cuenta o para restablecer su contraseña.*	

Microsoft Teams		
Función de chat	**Publicar en un canal Teams**	**Llamadas**
No disponible	Parcialmente disponible	No disponible
Las conversaciones entre alumnado en Microsoft Teams solo se permitirán si se cuenta con la autorización por escrito del equipo directivo y del equipo regional de TI, previa solicitud enviada al servicio de asistencia técnica de Cognita. Las conversaciones solo podrán tener lugar en grupos de Teams creados y supervisados por el	*El alumnado solo puede y debe publicar mensajes de Microsoft Teams en los espacios de los que forman parte y que hayan sido creados y sean gestionados por el profesorado.* *El alumnado no debe crear espacios en Microsoft Teams.*	*Se podrán autorizar las llamadas de alumnado dentro de Microsoft Teams siempre que se cuente con el permiso por escrito del equipo directivo (SLT) y del equipo regional de TI, mediante una solicitud enviada al servicio de asistencia técnica de Cognita. Las llamadas solo podrán realizarse dentro de*

profesorado.		*los grupos de Teams creados y supervisados por el profesorado.*

19.2 Se anima al personal a utilizar la plataforma de mensajería preferida de Cognita, Microsoft Teams. Sin embargo, si esta opción no es viable en determinadas circunstancias, se permite el uso de WhatsApp en un teléfono de trabajo, siempre que el personal:

- discutir cualquier cosa confidencial o sensible sobre los alumnos, padres y/o colegas (tenga en cuenta que nunca se debe compartir información relacionada con la protección a través de WhatsApp)
- enviar mensajes, GIFs y/o memes inapropiados, ofensivos y/o controvertidos (incluso si se consideran una 'broma')
- compartir datos personales y/o información comercialmente sensible
- unirse y/o crear grupos de WhatsApp creados por padres/tutores. Esto incluye a aquellos que son ambos padres y/o empleados de la colegio (hacerlo se considera un conflicto de intereses).

Aunque el uso de WhatsApp para el trabajo ofrece varias ventajas, debe ajustarse a nuestra política de protección de datos y a las normas generales en materia de conducta y profesionalidad. Por ello, el personal debe actuar con prudencia al utilizar esta aplicación en un teléfono de empresa y enviar únicamente mensajes que no les suponga ningún problema que se hagan públicos. Mantén una comunicación profesional, respetuosa y relacionada con el trabajo.

Nota: A partir de abril de 2025, Meta (la empresa matriz de WhatsApp) introdujo un asistente de IA integrado conocido como 'Llama 4' dentro de la plataforma de mensajería WhatsApp. Si bien esta función se describe como "opcional", no se puede eliminar de la interfaz de la aplicación.
Aunque no se recomienda el uso de Llama 4 en dispositivos de trabajo, no está explícitamente prohibido, ya que Cognita actualmente no tiene medios para desactivar la función. Los empleados que decidan interactuar con el asistente de IA deben hacerlo con precaución y en estricto cumplimiento de la **Política Global de IA de Cognita.**

En lo que respecta a la comunicación en línea entre el personal y los padres, la plataforma preferida y autorizada por Cognita es Microsoft Teams (MS Teams). Reconocemos la importancia de una comunicación digital eficaz, especialmente para las reuniones y conversaciones a distancia entre el personal y los padres. Sin embargo, esto conlleva ciertos riesgos, sobre todo en el cambiante panorama de la inteligencia artificial (IA), en el que las grabaciones y las transcripciones pueden ser manipuladas.

Para mitigar estos riesgos y mantener los estándares profesionales, deben seguirse las siguientes directrices a la hora de celebrar reuniones en línea con las familias.

En el caso de MS Teams

- Se debe hacer todo lo posible por utilizar esta plataforma para las reuniones o conversaciones en línea con las familias.
- La reunión debe ser iniciada internamente por un miembro del personal, asegurándose de que la persona que la inicia (el anfitrión) mantenga el control sobre la sesión.
- Las reuniones de MS Teams deben grabarse* (utilizando la herramienta del propio MS Teams y no productos de terceros), para disponer de un registro verificable en caso de que sea necesario más adelante.
- Queda estrictamente prohibido el uso de herramientas de transcripción externas o complementos. Se permite la función de transcripción integrada en MS Teams, que deberá utilizarse si la transcripción resulta necesaria.
- Debe mantenerse la profesionalidad en todo momento. En las reuniones que puedan implicar conversaciones delicadas o conflictivas, deberá estar presente un segundo miembro del personal, preferiblemente del Equipo Directivo (SLT), para ayudar a orientar el debate de forma tranquila y constructiva.

*Antes de la grabación, se recomienda que el personal lea el aviso legal que figura en el Apéndice C: Aviso legal para las familias sobre la comunicación a través de Microsoft (MS) Teams.

En el caso de otras plataformas de videoconferencia

No se permite utilizar otras plataformas de videoconferencia salvo que hayan sido aprobadas mediante una DPIA. También deberán cumplirse las condiciones anteriores y, si por cualquier motivo no fuera posible, deberá notificarse a servicedesk@cognita.com o consultarse con el equipo regional de TI.

Cognita sabe que algunos colegios utilizan TES Parents Evening System para celebrar reuniones en línea entre las familias y el profesorado. A fecha de agosto de 2025, esta plataforma no ofrece servicio de transcripción ni permite grabar. Debe tenerse en cuenta que, por tanto, no quedará un registro de la conversación —por ejemplo, de lo dicho y de quién lo dijo— al que pueda recurrirse posteriormente. Esto no autoriza a transcribir o grabar las llamadas por otros medios, lo cual está prohibido. Cognita también sabe que la plataforma permite que las familias inicien llamadas; esta práctica también está prohibida.

20 Supervisión de la actividad en línea del alumnado (incluyendo correo electrónico)

Cognita reconoce la importancia de garantizar la seguridad de los/las niños/as en Internet. Por ello, nos reservamos el derecho a supervisar la actividad en línea de los/las alumnos/as, incluidas sus cuentas de correo electrónico. Esto es especialmente aplicable en casos en los que se sospeche o se denuncie alguna actividad inusual, insegura o inapropiada.

Del mismo modo, también somos conscientes de la autonomía de los/las alumnos/as y de su derecho a la privacidad de los datos, especialmente entre el alumnado de más edad. Por lo tanto, cualquier supervisión en línea se llevará a cabo de manera razonable y proporcionada, con una justificación clara de por qué se lleva a cabo. En resumen, el objetivo de Cognita es equilibrar la privacidad del alumnado con nuestra responsabilidad (y deber de cuidado) de protegerlos y supervisarlos en Internet.

Este enfoque también se extiende a la supervisión llevada a cabo por las familias. Aunque Cognita no puede controlar la naturaleza de la supervisión fuera de la colegio (por ejemplo, en el hogar), animamos a las familias a que consideren cuidadosamente las circunstancias en las que supervisan la actividad en línea de sus hijos/as, incluida su correspondencia por correo electrónico. Una vez más, dicha supervisión debe ser razonable y proporcionada, teniendo en cuenta la edad, la madurez y el derecho a la privacidad de los menores.

21 Uso de drones

Los drones son cada vez más populares para capturar imágenes. Sin embargo, su uso debe cumplir con la normativa local (por favor, consulta la normativa correspondiente a tu región), así como con los procesos internos del grupo Cognita.

Se debe solicitar permiso al Responsable de Salud y Seguridad – Europa y Estados Unidos. Si se concede el permiso para el uso de un dron, deberá realizarse una evaluación de riesgos exhaustiva.

Desde la perspectiva de la privacidad de los datos, se deben tomar todas las medidas posibles para evitar:

- capturar cualquier elemento identificable, como (pero no limitado a):
    - sujetos de datos (personas, incluyendo su imagen y/o voz), matrículas de vehículos
- hacer volar drones cuando haya personas en el lugar
- hacer volar drones cerca de ventanas/entradas, aparcamientos, etc. (donde es más probable que haya elementos identificables)

Si se hace volar un dron cuando hay personas presentes, este hecho se debe comunicar claramente a dichas personas con antelación y hacerles conscientes de la iniciativa, para que puedan dar su permiso (consentimiento) o manifestar su objeción a ser grabadas. También se les debe dar la oportunidad, con suficiente antelación, de plantear cualquier duda y/o preocupación.

Si se capturan imágenes con dron y se almacenan localmente (por ejemplo, en una tarjeta SD), y si dichas imágenes incluyen datos identificables, el centro debe asegurarse de que la tarjeta SD se mantenga segura en todo momento. Debe permanecer en el centro, y las imágenes deben eliminarse una vez hayan cumplido su propósito.

Si las imágenes se almacenan en software de terceros (por ejemplo, mediante una solución en la nube), dicho software debe ser evaluado por Cognita a través del proceso de Evaluación de Impacto en la Privacidad de los Datos (DPIA).

Desde la perspectiva de la seguridad, los drones no deben utilizarse para interferir con las medidas y/o operaciones de seguridad del centro, ni volarse de forma que comprometa la seguridad.

También existen varias consideraciones importantes en materia de salud y seguridad

respecto al uso de drones – por favor, consulta la **Política de Gestión de Instalaciones** para más información.

22 Uso de dispositivos inteligentes y seguimiento de usuarios

El uso de dispositivos inteligentes no está permitido en presencia de menores. Cognita no aprueba el uso de dispositivos de rastreo durante el horario lectivo y/o en actividades del colegio, como visitas educativas o actividades extraescolares. Los colegios ya cuentan con medidas de seguridad y protección para garantizar la seguridad del alumnado, tanto dentro como fuera del centro.

No obstante, reconocemos que, a medida que la tecnología permite a los padres y a las madres rastrear los movimientos de sus hijos/as mediante dispositivos inteligentes, algunos/as pueden optar por utilizar esta funcionalidad con mayor frecuencia, por ejemplo, cuando sus hijos/as se encuentran fuera del recinto del colegio, como en una excursión. La decisión de utilizar esta tecnología recae en las familias.

Algunos de los argumentos a favor de su uso incluyen

- las familias tienen derecho a saber dónde están sus hijos
- las familias perciben que esta tecnología puede ayudar a mantener a sus hijos/as más seguros/as
- la tecnología proporciona tranquilidad a las familias

Sin embargo, existen diversas implicaciones éticas y de seguridad que las familias pueden no considerar antes de optar por rastrear a sus hijos/as mediante un dispositivo inteligente. En última instancia, se recomienda a las familias que equilibren la seguridad con la libertad personal, teniendo en cuenta múltiples variables, como, por ejemplo:

- la edad de los menores
- su capacidad cognitiva, madurez y nivel de comprensión
- la ubicación, por ejemplo, del destino de la excursión (si es especialmente remoto o se percibe como de mayor riesgo)

Por ello, es posible que los colegios detecten dispositivos de rastreo como AirTags integrados en las pertenencias y/o ropa del alumnado. En estos casos, se debe hablar con las familias y recordarles que:

- esta tecnología no está diseñada para rastrear los movimientos de personas, sino de objetos o pertenencias
- Cognita no aprueba el uso de dispositivos de rastreo durante el horario lectivo y/o en actividades del colegio, como visitas educativas o actividades extraescolares
- el uso de rastreadores puede generar una falsa sensación de seguridad; los menores pueden quitar el dispositivo, cambiarlo de lugar o incluso perder el objeto en el que está colocado

Puede resultar difícil para los centros prohibir el uso de dispositivos de rastreo (excepto aquellos integrados en teléfonos móviles – consulta la Política sobre el uso de móviles). No obstante, en el caso de otros dispositivos como los AirTags, puede ser útil que los centros orienten a las familias hacia este artículo.

23 Anexo A- Declaración sobre Filtrado 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.

Nuestros sistemas de filtrado de web 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

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

ACUERDO DE USO DEL iPAD/LAPTOP 1:1 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 1:1. 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 solo 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.

SÉ 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:

25 Apéndice C – Aviso legal para los padres sobre la comunicación a través de Microsoft (MS) Teams

Aviso legal que debe leerse en voz alta a los padres antes de que comience la reunión:

«Antes de comenzar, me gustaría informarles de que esta reunión se celebra a través de Microsoft Teams, que es nuestra plataforma de videoconferencia preferida. Esto se ajusta a nuestra política interna, que exige que todas las sesiones entre el personal y los padres se celebren en Microsoft Teams.

Al iniciar la llamada desde nuestro lado, podemos mantener un control adecuado de la sesión de acuerdo con nuestros procedimientos de protección y seguridad de datos.

Tengan en cuenta también que esta reunión se grabará. La grabación, junto con una transcripción generada automáticamente, se almacenará de forma segura y podrá consultarse más adelante si fuera necesario. Esto se hace para garantizar la transparencia y facilitar el mantenimiento de registros precisos.

Si tiene alguna duda al respecto, no dude en plantearla ahora, antes de que continuemos.»

26 Anexo C – Políticas relacionadas

Europa y Estados Unidos

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

Group IT

- Group Policy - Software (Applications)
- Cognita Password Policy
- Personal and Professional Boundaries Policy
- Cognita Cyber Security Policy
- Cognita Safeguarding Systems Cyber Security Policy

27 Anexo D – Recursos en línea

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 consulta	
Patrocinador/aprobador de documentos	Head of IT – Europe and United States
Document author	Head of IT – Europe and United States
Consultado con	Europe Digital Learning Advisors
	Group Cyber Security
	Europe IT POD Leads
	Regional Safeguarding Lead - Europe and United States
Audiencia	
Audiencia	Personal
	Alumnado y familias
	Proveedores
	Visitantes
	Contratistas
Aplicación del Documento	
Esta política está relacionada con esta jurisdicción	Todos los colegios y oficinas de Cognita Europe
Control de versiones	
Ciclo de revisión	Anual
En vigor desde	1 septiembre 2026
Próxima fecha de revisión	30 junio 2027
Version	1.2 EMITIDO