Política de Uso Aceptable y Seguridad Digital

ESPAÑA

Septiembre 2023

1 Introducción

1.1. El uso de la tecnología como herramienta se ha convertido en parte integral del entorno escolar y del doméstico.

1.2. Cognita Schools se compromete a un uso efectivo y apropiado de la tecnología para la docencia, el aprendizaje y la administración del colegio, así como a proteger al personal, a los alumnos, a los padres y a los visitantes de cualquier uso ilegal o lesivo de la tecnología por parte de individuos o grupos de individuos, sea o no deliberado.

1.3. El colegio fomenta activamente la participación de los padres para que contribuyan a proteger el bienestar de los alumnos y a un uso seguro de la tecnología.

1.4. La presente política rige para el uso de:

- Todos los dispositivos y equipos tecnológicos conectados a la red del colegio.
- Todos los dispositivos tecnológicos facilitados por el colegio a empleados y contratistas, ya sea en sus instalaciones o fuera de ellas.
- Todos los dispositivos tecnológicos facilitados por el colegio a los alumnos mediante el programa de dispositivos 1 a 1, ya sea en sus instalaciones o fuera de ellas.
- Todas las aplicaciones y servicios informáticos provistos por el colegio para las tareas administrativas y de docencia y aprendizaje.
- Todas las aplicaciones y servicios informáticos disponibles en línea y accesibles mediante la red del colegio o un dispositivo tecnológico de este.

1.5. Esta política está disponible en la página web del colegio y se facilitará una copia de la misma al personal, a los alumnos, a los padres y a los visitantes que la soliciten.

1.6. En caso de incumplimiento de esta política y sus obligaciones, el hecho de no haberla leído no se aceptará como defensa o excusa.

2 Finalidad de la presente política

2.1 Promover el uso responsable y cuidado de la tecnología así como de los servicios informáticos disponibles para miembros del personal, alumnos, padres y visitantes.

2.2 Indicar los usos aceptables e inaceptables de la tecnología y los servicios informáticos del colegio, ya sea en sus instalaciones o fuera de ellas.

2.3 Describir las funciones y responsabilidades de los miembros del personal, alumnos, padres y visitantes.

2.4 Informar a los alumnos y animarlos a hacer un buen uso de las oportunidades educativas que les brinda el acceso a la tecnología en el colegio.

2.5 Proteger y promover el bienestar de los alumnos, en particular anticipando y evitando los riesgos derivados de:

- la exposición a contenido dañino o inapropiado (como material pornográfico, racista, extremista u ofensivo);
- un contacto indebido con extraños;
- ciberacoso y el maltrato;
- la posibilidad de que se copien y compartan datos e imágenes personales,

2.6 Describir los procedimientos de supervisión y filtrado digital en los dispositivos y la red del colegio.

2.7 Exponer los requisitos para informar de un uso indebido de la tecnología.

2.8 Asegurar que todos los interesados, incluyendo SLT, CPC e IT tengan oportunidad de colaborar.

3 Ámbito de aplicación

3.1 La presente política aplica a todos los miembros del personal, alumnos, padres y visitantes del colegio.

3.2 El colegio adoptará un enfoque amplio y deliberado a la hora de determinar qué se considera tecnología. Esta política se refiere a toda la tecnología, dispositivos informáticos y de comunicaciones, programas, equipos de redes, servicios y aplicaciones asociados. Esto incluye:

- la red del colegio, el wifi y el acceso a Internet;
- tabletas, ordenadores de sobremesa, portátiles y dispositivos de cliente ligero;
- teléfonos móviles e inteligentes; relojes inteligentes;
- dispositivos digitales de sonido, imágenes fijas o en movimiento (p. ej., reproductores de música personales y dispositivos GoPro);
- pantallas y pizarras digitales;
- impresoras 2D y 3D;
- aplicaciones de comunicación y colaboración (p. ej., correo electrónico y Teams);
- entornos de aprendizaje virtual;
- aplicaciones de mensajería móvil (p. ej., Snapchat y WhatsApp);
- redes sociales (p. ej., Facebook, Instagram, TikTok),

3.3 Esta política aplica al uso de la tecnología tanto en las instalaciones del colegio como fuera de ellas.

3.4 Rige también para cualquier miembro de la comunidad escolar en aquellos casos en los que se ponga en riesgo la cultura o la reputación del colegio.

3.5 Asimismo, es de aplicación para cualquier miembro de la comunidad escolar cuando esté en juego la seguridad de un miembro del personal, alumno, padre o visitante.

4 Documentación relacionada

4.1 Política para la protección integral de menores

4.2 Política de prevención del extremismo y la radicalización

4.3 Política de comportamiento

5 Funciones y responsabilidades

5.1 La presente política es responsabilidad del Cognita Regional Director of Education.

5.2 El director del colegio es el encargado de su publicación, así como de asegurar su implantación y supervisión continuas.

5.3 El responsable europeo de TI de Cognita es el responsable de garantizar que la tecnología y los servicios informáticos se desplieguen y supervisen de acuerdo con esta política

5.4 El Responsable de Ciberseguridad es responsable del proceso de filtrado de contenidos y monitorización de actividad.

5.5 El Coordinador de Protección y Bienestar es responsable de la protección del menor y seguridad digital que podría incluir la supervisión y acción en los siguientes aspectos:

- Informes sobre el filtrado de contenidos y monitorización de actividad.
- Preocupaciones relativas a la protección del menor
- Comprobaciones de los sistemas de filtrado de contenidos y monitorización de actividad

5.6 Asimismo, deberán atenerse a ella todos los miembros del personal, alumnos, padres y visitantes.

6 Uso seguro de la tecnología

6.1 El colegio se compromete a un uso efectivo y apropiado de la tecnología para las tareas administrativas, de docencia y aprendizaje.

6.2 La tecnología deberá usarse de un modo seguro, responsable, legal y respetuoso con los demás. Los miembros del personal, alumnos, padres y visitantes serán en todo momento responsables de sus acciones, su conducta y su comportamiento al utilizar dicha tecnología.

6.3 El colegio apoyará el uso de la tecnología y facilitará un acceso a Internet con las mínimas restricciones, siempre y cuando sea posible y necesario, sopesando siempre las necesidades educativas de los alumnos, la seguridad y bienestar de estos y de los miembros del personal, padres y visitantes, así como la seguridad e integridad de nuestros sistemas.

6.4 Disponemos de herramientas de monitorización y alerta para mantener la seguridad y protección de alumnos, personal, padres y visitas.

6.5 Las herramientas de filtrado de contenidos y monitorización de actividad se revisan anualmente para asegurar que cumplen las necesidades de nuestros alumnos y personal. En esta revisión están implicados departamentos de IT, Ciberseguridad, Directores y la Propiedad.

6.6 En aras de asegurar la protección del menor, los dispositivos 1 a 1 de los alumnos cuentan con programas de supervisión y control preinstalados. Dichos programas proporcionan datos históricos y en tiempo real sobre el uso del dispositivo (p. ej., la navegación por Internet). La información recopilada se guarda por un periodo de 90 días. Para más información sobre cómo tratamos los datos personales que recopilamos, consulte la declaración de confidencialidad del colegio, disponible en su página web. Para más información sobre el filtrado de contenido y monitorización de actividad en los colegios Cognita, véase la Declaración de Filtrado Web (Anexo B).

6.7 El software de monitorización usa la Inteligencia Artificial (IA) para determinar el filtrado de contenidos en páginas web de nueva creación , así como su categorización.

6.8 Los técnicos informáticos pueden hacer cambios manuales en el sistema de filtrado.

6.9 El Coordinador de Bienestar y Protección debe entender los sistemas de monitorización implementados. Reciben formación a este efecto para tener la capacidad de analizar de los datos de filtrado.

6.10 Todo el personal del centro, así como los responsables de Gobernanza reciben formación en ciberseguridad cada año.

6.11 Todo el personal debe entender que el sistema de filtrado de contenidos existe para salvaguardar a los menores, así como las expectativas y requisitos asociados a éste.

6.12 El colegio puede hacer cambios a medida al sistema de filtrado de contenidos, así cómo en el acceso a la tecnología, para aquellos alumnos que potencialmente pudieran encontrarse en una situación de riesgo.

6.13 Queremos que los alumnos disfruten del uso de la tecnología y que se conviertan en usuarios competentes de la misma, puesto que esta se ha convertido en parte fundamental de la educación, no solo como instrumento para ofrecer una docencia y un aprendizaje de calidad, sino también como plataforma de colaboración y productividad.

6.14 Se inculcará a los alumnos la importancia del uso seguro y responsable de la tecnología para ayudarles a protegerse a sí mismos y a los demás en el entorno virtual.

6.15 El colegio promueve activamente la participación de los padres para que éstos contribuyan a fomentar un uso seguro de la tecnología entre sus hijos.

6.16 Cualquier causa o hecho que pudiera generar inquietud debido a un uso no seguro o inadecuado de la tecnología, deberá notificarse a un profesor, al director o al Coordinador de Bienestar y Protección.

6.17 El director del colegio deberá comunicar cualquier incidente grave relacionado con un uso no seguro o inadecuado de la tecnología al director europeo de TI de Cognita, quien lo registrará e investigará.

6.18 Los recursos siguientes pueden ser de utilidad para todos los usuarios de la tecnología a la hora de protegerse en el entorno virtual:

- UK Safer Internet Centre [Centro de Reino Unido para un Internet más seguro]
- Internet Matters - recursos
- Centro de seguridad para las familias de Google
- Common Sense Media

7 El derecho a utilizar la red y los equipos del colegio

7.1 Se asignará un nombre único de usuario y una contraseña a los empleados y alumnos del colegio para que accedan a los dispositivos y servicios tecnológicos.

7.2 Algunos recursos compartidos tendrán un nombre de usuario y contraseña genéricos para su acceso.

7.3 Toda la tecnología del colegio será propiedad del centro educativo.. El colegio podrá, de forma razonable, reclamar los dispositivos entregados a personal o alumnos, revocar el acceso a los servicios tecnológicos del centro en cualquier momento y, si procede, solicitar la devolución del-dispositivo al colegio.

7.4 Solamente deben conectar a la red interna del colegio equipos que formen parte de ésta; los dispositivos personales deberán conectarse únicamente a la red de invitados.

7.5 Queda prohibido cualquier intento, por parte de un miembro del personal, estudiante, padre o visitante, de utilizar o acceder a una cuenta de usuario o dirección de correo electrónico para los que no se disponga de autorización.

7.6 Se podrán facilitar dispositivos designados a los empleados del colegio y los estudiantes con fines administrativos, docentes o de aprendizaje:

- Los estudiantes a los que se les haya proporcionado un dispositivo 1 a 1 deberán firmar el acuerdo de uso del portátil/iPad (véase el anexo A).
- Los estudiantes que dispongan de un dispositivo designado podrán utilizarlo durante las clases siguiendo las indicaciones del profesor.
- Los empleados y alumnos del colegio son responsables de la seguridad y la protección del dispositivo designado cuando lo saquen del centro.
- Los dispositivos facilitados por el colegio, junto con sus periféricos correspondientes, deberán devolverse en buenas condiciones (lo cual excluye el desgaste habitual por uso) y en buen estado de funcionamiento.
- Los empleados o los padres son los responsables del coste que suponga sustituir el dispositivo asignado por uno del mismo tipo en caso de que se haya perdido o se haya dañado de forma intencionada o por negligencia.

7.7 El colegio pone a disposición de empleados y alumnos dispositivos comunes para tareas generales, para su uso en las aulas o para aplicaciones especializadas.

7.8 Ni los empleados ni los alumnos del colegio podrán acceder o intentar acceder a recursos informáticos que estén asignados a otra persona salvo que cuenten con una autorización expresa

7.9 Por motivos de seguridad, los usuarios deben cerrar sesión o cerrar sus dispositivos cada vez que dejan de usarlos. Deben cerrar sesión y apagar los dispositivos al final del día.

8 Uso adecuado de la tecnología para la seguridad digital

8.1 El colegio proporciona **cuentas de aplicaciones o del sistema** para el personal, los alumnos, los padres y para invitados cuando sea necesario.

- Normativa al respecto:
  - No se puede ceder el uso de la propia cuenta a terceros.
  - No se puede utilizar una cuenta de terceros.
  - Se debe bloquear el dispositivo o cerrar la sesión en la cuenta cuando este no esté en uso.
  - Solo se utilizarán las aplicaciones y el correo electrónico del colegio para asuntos oficiales o para acceder la correspondencia digital del colegio.
  - No se podrán enviar mensajes o correos electrónicos desde cuentas del colegio que finjan provenir de una persona diferente al remitente real.

El personal y los alumnos deben:

- Usar cuentas oficiales del colegio en plataformas colaborativas aprobadas.

8.2 El colegio proporciona **equipos y programas de software** para apoyar la docencia y a la administración del colegio.

- Se espera que los usuarios de los equipos tecnológicos del colegio tengan cuidado de estos usándolos de un modo responsable.
- Los dispositivos tecnológicos no deben sacarse de las instalaciones, exceptuando los casos en que:
  - El dispositivo esté asignado a un miembro individual del personal.
  - El dispositivo esté asignado a un alumno dentro del programa 1 a 1.
  - Medie un permiso por escrito de un miembro del equipo directivo del colegio.

- Los dispositivos tecnológicos del colegio asignados al personal o los alumnos son responsabilidad de éstos.
- Los equipos tecnológicos portátiles, incluyendo los dispositivos facilitados por el colegio, no deben dejarse desatendidos.
- En caso de pérdida o daño de un equipo tecnológico del colegio por parte de un alumno, deberá notificarse cuanto antes a un profesor, a un miembro del equipo directivo del colegio o del equipo de soporte informático.
- El robo de un dispositivo tecnológico del colegio asignado a un miembro del personal o un alumno en el marco del programa 1 a 1 deberá notificarse siempre a la policía~~,~~ así como a un profesor en el caso de que el robo lo haya sufrido un alumno, o bien a un miembro del equipo directivo del colegio o del equipo de soporte informático. Siempre será necesario presentar una la copia de la denuncia correspondiente.
- El uso indebido o el daño deliberado del equipo del colegio conllevará que el culpable deba asumir los gastos de sustitución del mismo en su totalidad.
- Está prohibido:
    - Intentar instalar programas en un dispositivo del colegio o facilitado por este más allá de aquellos especificados a través del centro de descargas del colegio (*Application Download Store*).
    - Descargar o acceder a programas ilegales en dispositivos del colegio.
    - Descargar paquetes de programas de la red del colegio a dispositivos portátiles o personales.
    - Intentar copiar o borrar programas de dispositivos del colegio o facilitados por este.
    - Intentar modificar la configuración del equipo informático o de los programas asociados si no es por indicación escrita del colegio.
    - Instalar plugins, extensiones o similares no autorizados en el navegador de los dispositivos del colegio
    - Utilizar programas que no requieren de instalación (aplicaciones portables) que permitan ejecutar aplicaciones no autorizadas, por ejemplo, juegos o clientes VPN

8.3 El colegio proporciona recursos tecnológicos para almacenar **datos** y acceder a ellos.

- Está prohibido:
    - Acceder o intentar acceder a datos sin tener autorización para ello.
    - Modificar o interferir con obras digitales pertenecientes a otros usuarios.
    - Compartir información privada, sensible o confidencial, al menos que:
        - Tienes permiso para compartir
        - El método de compartirla es seguro
- Al acceder a los datos, es responsabilidad de los usuarios estar familiarizados con las violaciones de los derechos de propiedad intelectual (lo que incluye derechos de autor, derechos de patentes y marcas y derechos morales).

8.4 El colegio se esfuerza por proteger frente a todos los riesgos de **seguridad** relacionados con la tecnología y, en la medida de lo posible, por mitigarlos.

- Utiliza sistemas de filtrado para bloquear el acceso a contenidos inadecuados dentro de lo posible y para proteger el bienestar y la seguridad de miembros del personal, alumnos, padres e invitados.
- Está prohibido:
  - Intentar evitar o deshabilitar los sistemas de filtrado del colegio cuando se estén utilizando dispositivos o la red de este.
  - Utilizar programas o sistemas de enrutamiento de red diseñados para esquivar los filtros y acceder a páginas bloqueadas.
  - Intentar esquivar los sistemas de seguridad tecnológica cuando se estén utilizando dispositivos o la red del colegio.
  - Utilizar programas o sistemas de enrutamiento de red diseñados para esquivar los sistemas de seguridad tecnológica del colegio.
- El acceso a contenidos inadecuados en un dispositivo o en la red del colegio deberá notificarse cuanto antes a un profesor o un miembro del equipo directivo del colegio o del equipo de soporte informático.
- El colegio dispone de sistemas de seguridad tecnológicos para bloquear y proteger frente a virus informáticos y otros programas maliciosos, como los programas espía.
- Cualquier motivo de inquietud referente a virus y otros programas maliciosos deberá notificarse cuanto antes a un profesor o un miembro del equipo directivo del colegio o del equipo de soporte informático.

8.5 Es responsabilidad de todos los usuarios proteger su **bienestar** y el de los demás tanto en los dispositivos personales como en los del colegio.

- Ciberacoso: a los alumnos les está prohibido utilizar la tecnología propia o la del colegio para acosar a otros.
- Extraños: asimismo, no pueden utilizar la tecnología propia o la del colegio para entablar contacto con personas desconocidas.
- Sexteo: a los alumnos les está prohibido utilizar la tecnología propia o la del colegio para crear o compartir contenido sexual ya sea en formato de imagen, audio, vídeo o texto.
- Cualquier motivo de inquietud sobre bienestar en relación con el uso de la tecnología deberá notificarse cuanto antes a un profesor, un miembro del equipo directivo del colegio o al Coordinador de Bienestar y Protección.
- Los miembros del personal nunca deben reenviar contenido inapropiado que haya recibido de un niño, padre o miembro del personal a ningún otro niño, padre o miembro del personal. En caso de recibir contenido de esta naturaleza, deberán notificarlo inmediatamente al CPC y al director.

8.6 El colegio proporciona un acceso apropiado a **Internet y a las redes sociales** como apoyo a la docencia y a la gestión del colegio.

- Internet brinda a los usuarios de la tecnología oportunidades nunca antes vistas de obtener información, conversar y contactar con personas, organizaciones y grupos de todo el mundo y así ahondar en competencias, conocimientos y habilidades.

- El colegio apoya activamente el acceso al mayor abanico posible de fuentes de información, así como el desarrollo de las competencias necesarias para filtrar, analizar, interpretar y evaluar la información hallada.
- Los miembros del personal, alumnos, padres y visitantes deberán abstenerse de utilizar un dispositivo o la red del colegio para visitar deliberadamente páginas de Internet de contenido obsceno, ilegal, agresivo, ofensivo, pornográfico, extremista, que incite al odio o que resulte inadecuado de cualquier otro modo.
- Asimismo, no se podrá utilizar el dispositivo o la red del colegio para acceder a páginas web de apuestas.
- Los miembros del personal, alumnos, padres y visitantes serán responsables de notificar a un miembro del equipo directivo el colegio, al Coordinador de Bienestar y Protección o al equipo de soporte informático cualquier material inadecuado al que se haya accedido desde un dispositivo o desde la red del colegio para que se pueda bloquear dicho acceso.
- En las redes sociales, se deberá reconocer y respetar en todo momento la privacidad del personal, los alumnos, los padres y los visitantes.
- Los miembros del personal no deben ponerse en contacto con ningún alumno menor de diecinueve años en cualquier red social o mediante el teléfono móvil personal.
- Los miembros del personal, alumnos, padres y visitantes del colegio deberán abstenerse de hacer comentarios ofensivos o inadecuados (incluyendo aquellos que desprestigien el nombre y la reputación del colegio) en cualquier foro o plataforma, como por ejemplo en las redes sociales, sea o no desde un dispositivo del colegio, cuando pueda establecerse una conexión entre el usuario y el colegio.

9 Dispositivos asignados por Cognita: Acceso y privacidad

9.1 Acceso a los dispositivos asignados y al contenido informático:

- Los dispositivos tecnológicos del colegio asignados al personal o los alumnos están únicamente destinados al uso por parte de la persona a quien se hayan asignado.
- En los dispositivos de los estudiantes puede instalarse una aplicación de gestión del aula con las funciones pertinentes para que el profesor controle y visualice la pantalla de los alumnos mientras dura la clase.
- En los dispositivos de Cognita pueden instalarse aplicaciones de soporte remoto que permiten que el equipo informático acceda a ellos para proporcionar asistencia remota, siempre con el permiso de la persona a quien esté asignado el dispositivo.
- Cognita se reserva el derecho a acceder a un dispositivo asignado y a supervisar su uso y su contenido en situaciones especiales entre las que se incluyen las siguientes:
  - Para detectar o evitar actos delictivos.
  - Para activar la protección de seguridad del sistema (p. ej., frente a virus, programas maliciosos, intentos de hackeo u otros riesgos).
  - Para investigar posibles usos indebidos, abusos o actividades ilegales.
  - Para supervisar el cumplimiento de las obligaciones legales y en materia de empleo.
  - Para garantizar la integridad de los dispositivos del colegio, la tecnología y los sistemas informáticos.
- Para que se pueda acceder a un dispositivo asignado, se debe otorgar permiso por escrito de la siguiente forma:
  - Lo otorgará el director o responsable de Recursos Humanos de Cognita para los dispositivos asignados a un miembro del personal.

  - Lo hará el director del colegio o el Coordinador de Bienestar y Protección para los dispositivos asignados a un alumno.
- Los datos presentes en un dispositivo de Cognita o a los que se haya accedido a través de este se rigen por las políticas de privacidad de Cognita y del colegio.

10 Fotografías e imágenes

10.1 El colegio cumple con la legislación en materia de protección de datos, es decir con el Reglamento General de Protección de Datos de 2018 (incluidas las modificaciones, ampliaciones o nuevas promulgaciones que se puedan producir del mismo) y entiende que una imagen o vídeo tienen la consideración de datos personales. Solicita el consentimiento de los padres para publicar imágenes o vídeos con fines de publicidad externa (como por ejemplo la página web) o con fines internos (como el anuario o un portal para padres). Los padres y tutores legales pueden revocar dicho consentimiento en cualquier momento informando por escrito al equipo administrativo del colegio.

10.2 El código de conducta para empleados de Cognita señala que Cognita no autoriza el uso de teléfonos móviles y cámaras personales por parte del personal en presencia de menores.

10.3 Los requerimientos de bienestar y seguridad para la etapa de educación infantil (*Early Years*) obligan a todos los colegios a disponer de una política clara sobre el uso de teléfonos y dispositivos móviles.

10.4 Los miembros del personal, alumnos, padres y visitantes no están autorizados a utilizar dispositivos tales como teléfonos móviles, relojes inteligentes, cámaras o grabadoras digitales para fotografiar o grabar en vídeo a miembros del personal o alumnos sin su permiso. El colegio podrá dar permiso en el caso de actuaciones o actos organizados por este.

10.5 Se pide a los padres que sean considerados a la hora de hacer vídeos o fotografías en actos del colegio y que no publiquen material de otros menores en cualquier plataforma pública sin el permiso de la familia en cuestión. Es ilegal vender o distribuir grabaciones de actos sin permiso. Si un padre no desea que, en un acto del colegio, otros asistentes graben o fotografíen a su hijo, deberá avisar al colegio de antemano y por escrito.

11 Uso de los equipos del colegio con fines personales

11.1 Los dispositivos y sistemas informáticos del colegio se proporcionan únicamente para tareas relacionadas con este: si alguien decide utilizar dichos equipos o sistemas informáticos con fines personales, deberá asumir que lo hace por cuenta y riesgo propios y que dicho uso podría considerarse un incumplimiento de la política de seguridad digital. Asimismo, conviene señalar que, de acuerdo con el punto 9 de la presente política, Cognita tendrá derecho a acceder a los equipos y la tecnología del colegio y a supervisar su uso y sus contenidos, lo cual incluye las comunicaciones que se hayan podido realizar a través de ellos.

11.2 En los dispositivos del colegio, solo se podrán instalar programas y aplicaciones autorizados.

11.3 Los dispositivos y la red del colegio no pueden utilizarse para llevar a cabo actividades comerciales ilegales.

11.4 Realizar transacciones económicas y privadas en equipos compartidos comporta un riesgo y compromete la seguridad de los datos personales.

12 Uso de dispositivos personales en el colegio

12.1 Los dispositivos personales no podrán conectarse a la red del colegio más que a través de la red wifi para invitados.

13 Procedimientos de notificación

13.1 Los miembros del personal, alumnos, padres y visitantes del colegio que tengan algún motivo de inquietud o hayan sufrido un incidente en relación con la tecnología deberán adoptar las medidas siguientes:

- Poner fin al problema o desactivar la tecnología en cuestión.
- Evitar la exposición de otras personas al incidente.
- Registrar la naturaleza del incidente y las personas afectadas.
- Preservar los elementos de prueba para permitir investigaciones cuando proceda.
- Informar del incidente o del motivo de inquietud a un profesor, al director del colegio, al Coordinador de Bienestar y Protección o al equipo de soporte informático, según proceda
- No iniciar una investigación al menos que tengan la autorización para hacerlo
- Completar un SIRF (informe de incidente serio)

13.2 Cualquier motivo de inquietud por un uso inseguro o inadecuado de la tecnología o por alguna cuestión de bienestar en relación con esta deberá notificarse a un profesor, al director o al Coordinador de Bienestar y Protección.

13.3 Los miembros del personal saben que deben reportar un incidente cuando:

- Son testigos de o sospechan que ha habido acceso a material no apropiado
- Son capaces de acceder a material no apropiado
- Incluyen en su docencia aspectos que podría crear actividad inusual en los registros de filtrado de contenido
- Hay un fallo en software o un abuso del sistema
- Perciben restricciones no razonables que afecten el aprendizaje y enseñanza o las tareas administrativas
- Se dan cuenta de abreviaciones o errores ortográficos que permiten acceso a material restringido

13.4 El acceso a contenidos inadecuados o cualquier motivo de inquietud relacionado con un virus u otro programa malicioso en un dispositivo o en la red del colegio deberá notificarse cuanto antes a un profesor o un miembro del equipo directivo del colegio o del equipo de soporte informático.

13.5 En caso de pérdida, daño o robo de un equipo tecnológico del colegio, deberá notificarse cuanto antes a un profesor o un miembro del equipo directivo del colegio o del equipo de soporte informático. Asimismo, el robo deberá comunicarse a la policía y se deberá obtener la copia de la denuncia correspondiente.

13.6 Los alumnos deben responsabilizarse del uso de sus equipos informáticos tanto en el colegio como en casa; si los padres o tutores legales albergan cualquier inquietud al respecto o detectan un problema, recomendamos que se pongan en contacto con el colegio cuanto antes para poder recibir orientación y ayuda.

13.7 El colegio tiene el deber de notificar cualquier motivo de inquietud grave a los equipos de seguridad y protección de las autoridades locales o a la policía, en cumplimiento de los requisitos legales.

14 Revocación de los derechos de acceso a la red y sanciones

14.1 En caso de violación de la política de seguridad digital en lo que respecta al uso de ordenadores, se podrán revocar los derechos de acceso a la red de la persona implicada, así como tomar otras medidas disciplinarias.

14.2 El colegio se reserva el derecho a denegar el acceso a la red en cualquier momento.

14.3 El colegio podrá informar a la policía o a cualquier organismo encargado de la aplicación de la ley si se da un uso que se considere que pudiera dar lugar a un procedimiento penal.

14.4 El colegio se toma muy en serio sus responsabilidades en relación con la seguridad digital y el uso de la tecnología por parte de empleados, alumnos, padres y visitantes y comprende la importancia de evaluar y revisar regularmente sus políticas y procedimientos y de hacer un seguimiento de los mismos.

15 Guía Adicional del uso del ordenador portátil/Ipad.,

15.1 ORDENADORES / IPADS

El alumno es el principal responsable del equipo que le entrega el colegio.

- Deberá hacer buen uso del equipo:
- Utilizará siempre su ordenador / IPad sobre una mesa escritorio y nunca en el suelo, silla etc…
- En ninguna circunstancia se podrá pintar o escribir en el equipo con tipp ex o producto similar.
- No podrá adherir pegatinas o adhesivos similares a menos que se trate de una pegatina (menos de 5cm) con el nombre del alumno.
- Cuando no se esté utilizando el equipo, deberá quedar guardado en la funda en la que se le entregó y el Ipad deberá permanecer cubierto con su tapa.
- Deberá cuidarlo y tratarlo con respeto en todo momento.
- El ordenador / iPad solo podrá contener las aplicaciones y software autorizado por el colegio. Solamente pudiendo acceder a sitios de naturaleza educativa y permitidas por el colegio. En el caso de dudar si un sitio o página es apropiado o no, el alumno podrá enviar su pregunta al departamento de IT (ithastings@hastingsschool.com).
- Cualquier problema o incidencia deberá comunicarse al departamento de IT vía email o en persona, independientemente de que afecte a su uso operativo o no (ithastings@hastingsschool.com).
- El equipo deberá traerse al colegio previamente cargado desde casa.
- El alumno podrá utilizar auriculares si el profesor lo autoriza y éstos no deberán ser inalámbricos.
- Se puede utilizar un ratón externo siempre y cuando sea compatible con el equipo. Cualquier otro dispositivo externo deberá ser validado por el departamento IT antes de su uso enviando un correo a (ithastings@hastingsschool.com).
- Todos los alumnos podrán conectarse a la wi fi “Cognita Students” siempre y cuando estén en el colegio. No se permite, en ninguna circunstancia el uso de otras redes.
- No se permite, en ninguna circunstancia el uso de VPN (Virtual Private Network).
- El alumno deberá bloquear su teclado cuando abandone su mesa, incluso por poco tiempo.
- En el caso eventual de que el colegio detecte que un alumno no utiliza adecuadamente su equipo, se le otorgará un punto negativo por uso inapropiado del mismo. Se informará a los padres y tutores a través de Cognita Connect. Los leaders de la dirección de bienestar monitorizarán la frecuencia de éstas conexiones de cada alumno y tomarán acciones en concordancia.

15.2 PASSWORDS

- El uso de passwords o claves para acceder al equipo deberán ser estrictamente personales y no transferibles. Los alumnos deberán mantenerlas de manera privada.
- En el caso de verse comprometida una clave deberá comunicarse el equipo de IT de manera inmediata.

LOS PASSWORDS SON CLAVES FIJAS Y NO PODRÁN SER CAMBIADOS POR LOS ALUMNOS.

15.3 ACCIDENTES / INCIDENTES

iPads

En caso de desperfecto o rotura, deberá reportarse al profesor o al director del colegio tan pronto como sea posible.Existen dos escenarios distintos:

- Si el alumno no tiene la culpa, el iPad se repara o se repone y los padres harán abono de 50 euros.
- Si el alumno se ve inculpado por descuido o negligencia, los padres abonarán el total de la reparación o reposición del equipo. En cualquier caso, la incidencia se analizará de manera individual. El fallo y sus consecuentes gastos se analizará, pero la decisión final será tomada por el colegio contra la cual no cabe ninguna apelación posterior al debate.

Laptops

En caso de desperfecto o rotura, deberá reportarse al equipo de IT de manera inmediata.En el caso de desperfecto del laptop caben dos escenarios distintos:

- Si el alumno no tiene culpa, el laptop se repara o se repone y los padres harán abono de 100 euros.
- Si el alumno tiene la culpa por descuido o negligencia, los padres abonarán el total de la reparación (475 euros) o reposición del equipo (1.100euros) . En cualquier caso, la incidencia se analizará de manera individual. El fallo y sus consecuentes gastos se analizará, pero la decisión final será tomada por el colegio contra la cual no cabe ninguna apelación posterior al debate.

15.4 ROBO/PÉRDIDA Y DEVOLUCIÓN

En el caso de pérdida o robo de un equipo, deberá reportarse al departamento IT de manera inmediata ya que cabe la posibilidad que se pueda localizar.

Si el equipo se pierde, los padres deberán abonar el coste total para reemplazarlo.

Si el equipo fuese robado, la familia deberá denunciarlo en la policía. Se valorarán los gastos del reemplazo. En el caso que el alumno no tuviera culpa alguna, eje; robo en una taquilla cerrada se repone el equipo con coste de 50 euros / 100 euros igual que se ha mencionado anteriormente. En el caso de que el equipo haya sido robado por negligencia del alumno, los padres se harán cargo de la totalidad.

Los alumnos mayores, en particular, NO DEBERÁN sacar los equipos del colegio en la hora del almuerzo. Deberán dejarlos guardados en sus taquillas. Igualmente, no deberán llevarse los equipos consigo si se van a ir a socializar con amigos. Reiteramos que la decisión final sobre quien recae la culpa será tomada por el colegio, no pudiendo ser motivo de apelación.

Todos los equipos deberán devolverse antes de que el alumno abandone Hastings, en su defecto se cobrará la totalidad del importe del reemplazo del equipo.

15.5 BOLÍGRAFOS Y CARGADORES

Los bolígrafos gráficos y cargadores no tienen cobertura y de ser extraviados, robados o rotos (de manera deliberada o accidental) deberán ser abonados en su totalidad. Se da la opción a los alumnos de no aceptar los bolígrafos para evitar este caso, pudiendo utilizar

bolígrafo compatible. Cualquier otro accesorio externo deberá ser validad por el departamento de IT, comunicándolo por correo (ithastings@hastingsschool.com).

15.6 REGULACIÓN DEL USO MÓVILES

Los alumnos de año 7 – 11 apagarán sus móviles antes del comienzo del horario escolar y los podrán encender nuevamente al abandonar el colegio. Si necesitasen llamar a casa, utilizarán el teléfono del colegio.

Los alumnos de año 12 y año 13 tiene permiso para utilizar sus móviles en el recreo y durante el almuerzo solamente.

Solamente se podrá hacer uso del teléfono móvil dentro del colegio si hubiera una necesidad médica.

Tampoco está permitido el uso del móvil durante excursiones o visitas sin la autorización de un miembro de staff a cargo del grupo.

Los teléfonos que se utilicen dentro del colegio sin permiso serán confiscados y custodiados en la recepción del edificio hasta finalizar el día (no después del almuerzo). Estos incidentes se anotarán en nuestro sistema SIMS como “uso de teléfono móvil” y llegará de manera automática un aviso a los padres.

15.7 OTROS DISPOSITIVOS PERSONALES

No se permite el uso de ningún otro dispositivo personal dentro del colegio independientemente de que sea de uso educativo o no

Appendix A1: Pupil 1-to1 iPad Consent Form

HASTINGS SCHOOL

IPAD AGREEMENT

Your iPad will be an exciting and integral part of the learning experience at school. Treat it with care and use it to collaborate with your classmates in a purposeful way that supports your learning journey. We've listed some simple guidelines below. Have a read and make a firm commitment to look after it and keep yourself and your classmates safe whilst working in the virtual environment.

BE SAFE

- Only visit websites that support the learning goals assigned by your teachers
- Use your device to collaborate on learning tasks and always remember to engage with others as if the conversation were happening face to face. Be kind and respectful at all times Do not use old Teams chats to contact pupils out of school time.
- Your device has all the necessary apps and software required for you to learn and work effectively. There is no need to install anything else or change any of the settings.
- Do not download or install any software, including browser plugins or VPNs, or change any of the settings configured by default.

BE RESPONSIBLE

- Keep your iPad safe when you are on the move, use the protective sleeve provided.
- Lock your iPad away when it's not with you.
- Do not decorate your iPad in any way.
- Handle your iPad with care, keeping it away from food and liquids
- Report any damage or problems to your Class Teacher/Building Leader straight away. Failure to do so will be seen as neglect.
- Any damage will be investigated. Your parents will have to pay 50€ to repair the damage or even more if it was your fault. This applies to both your iPad and iPads belonging to others.
- This also applies to pens and chargers.

If you or your parents would like for your iPad to stay in school, please make sure the charging cable is kept with the iPad and left in the charging cabinet in your classroom.

I agree to take very good care of my iPad by keeping it safe, and always being responsible and respectful of others in my words and actions when using it.

Student Name: _____Apple iPad Serial No:_____

Signature: _____

Date: _____

Appendix A2: Student 1-to1 Laptop Consent Form

HASTINGS SCHOOL

LAPTOP USAGE AGREEMENT

Your laptop is an important part of the learning experience at school. Please read the guidelines below. Make a firm commitment to look after it and keep yourself and your classmates safe whilst working in the virtual environment.

Student Name: _____Form:_____ HP Laptop Serial No:_____

BE SAFE

- Only visit websites that support the learning goals assigned by your teachers.
- Remember to always engage with others as if the conversation were happening face to face. Be kind and respectful.
- Your device has all the necessary apps and software required for you to learn and work effectively. You are only allowed to install apps from the Company Portal, if/when instructed by a member of staff. Otherwise, do not download or install any software, including browser plugins or VPNs, or change any of the settings configured by default. You may be subject to disciplinary action if you attempt to circumvent the controls.
- Only use the school WIFI to access the internet.
- Do not bring your own device to school.

BE RESPONSIBLE

- Keep your laptop safe when you are on the move, use the protective sleeve provided and keep it in your bag.
- Lock your laptop away when it's not with you. Do not take your laptop out of school at lunchtime or when you are socialising with friends.
- Handle your laptop with care keeping it away from food and liquids.
- Do not decorate your laptop in any way.
- Report any damage or problems immediately. Failure to do so will be seen as neglect.
- Any damage/loss will be investigated. If it is found not to be your fault, there will be an excess of 100€ to pay. If you have been found to cause damage /loss through intent or wilful neglect, parents will be charged for the cost of the laptop repair (475€) or replacement (1100€). This applies to both your laptop and other laptops. Pens and chargers are not covered and must be replaced.
- I have read and agree to all of the points above. I understand that I may be liable for the damage or loss of the laptop, pens and chargers.

Name: _____

Year Group/Class: _____ Date: _____

Anexo B: Declaración de Filtrado de Contenidos Web - Sep 2023

Esta declaración ofrece información detallada sobre las medidas adoptadas para filtrar y controlar el uso de Internet en los colegios Cognita.

Todo el uso de Internet en el centro se filtra y se 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 los menores. Por defecto, Google y Bing 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 cuenta con filtrado web desde los cortafuegos Watchguard y Fortinet Firewalls. Se aplican políticas específicas de filtrado web a distintos grupos por centro (por ejemplo, personal, Bachillerato, Primaria y Secundaria). Watchguard y Fortinet analizan el tráfico en función de un conjunto de políticas configuradas para el centro y permiten o bloquean el acceso a los sitios web en función de su categorización y contenido.

Todos los dispositivos 1to1 de los estudiantes 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 Watchguard como Fortinet y 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.

Enlace a Monitoring Provider Checklist Reponses (respuestas de la lista de comprobación del proveedor de supervisión de Lightspeed (2021)), que destaca hasta qué punto nuestra herramienta de filtrado bloquea los contenidos nocivos e inadecuados, sin afectar de forma injustificada a la enseñanza y el aprendizaje.

Los responsables de la protección de los menores y los directores de los centros escolares son los encargados de utilizar la información facilitada para adoptar las medidas oportunas. Los miembros del equipo central de Cognita están a su disposición para ayudarles con los problemas que requieran una intensificación.

Contactos clave:

- Jefe de Ciberseguridad, Cognita
- Responsable regional de seguridad, Europa y EE.UU.
- Director de Operaciones, Europa y EE.UU.

Appendix C: Filtrado de Contenidos y Monitorización de Actividad. Recursos útiles.

Department for Education
Keeping Children Safe In Education (DfE)
Meeting digital and technology standards in schools and colleges (DfE)
Broadband internet standards for schools and colleges (DfE)
Cyber security standards for schools and colleges (DfE)
Data protection policies and procedures (DfE)
Home Office
The Prevent duty: safeguarding learners vulnerable to radicalisation (Home Office)
Information Commissioner's Office
Data Protection Impact Assessment (DPIA) (ICO)
London Grid for Learning (LGfL) Online
Safety Audit (LGfL)
South West Grid for Learning (SWGfL)
Online Safety Review (360Safe) (SWGfL)
National Cyber Security Centre
Cyber security training for school staff
UK Safer Internet Centre
2023 Appropriate filtering and monitoring definitions published (UK Safer Internet Centre)
Test Your Internet Filter (UKSIC / SWGfL)
Filtering provider responses - self-certified by service providers (UKSIC)
A Guide for education settings and filtering providers (UKCIS)
Establishing appropriate levels of filtering (UKSIC)
Online safety in schools and colleges: questions from the governing board (UKCIS)
Digital Resilience
HeadStart Online Digital Resilience Tool (HeadStart Kernow)

Version control:

Ownership and consultation	
Document Sponsor	Cognita Regional Director of Education
Document Author / Reviewer	COO Europe and USA Reviewed by Head of Digital Learning June 2023 Reviewed by Regional Safeguarding Lead- June 2023 Reviewed by Head of Cyber Security- June 2023 Head IT Spain & Italy August 2023
Consultation & Specialist Advice	
Document application and publication	
England	No
Wales	No
Spain	Yes
Switzerland	No
Italy	No
Version control	
Current Review Date	September 2023
Next Review Date	September 2024
Related documentation	
Related documentation	Safeguarding and Child Protection Policy Preventing Radicalisation and Extremism Policy Behaviour Policy