

2026/2027

Política de Seguridad en Internet y Dispositivos Electrónicos

WHOLE SCHOOL



SINCE 1973

Responsable de la política:

Director del colegio

1. Objetivo y Ámbito de Aplicación

Morna International College se compromete a promover un uso seguro, responsable y saludable de la tecnología. Esta es la política principal del colegio sobre seguridad en internet y dispositivos electrónicos, y establece normas de obligado cumplimiento para alumnos, personal, padres y tutores, visitantes y otros miembros de la comunidad escolar.

A efectos de esta política, «seguridad en internet» se refiere a las medidas de protección, uso responsable y seguridad aplicables a la tecnología digital, los servicios en línea, las comunicaciones electrónicas, las cuentas y los dispositivos. El término inglés e-safety se mantiene en el título original de la política por continuidad, pero tiene el mismo significado que «seguridad en internet» en esta política y en los documentos relacionados del colegio. La política abarca los dispositivos propiedad del colegio y los personales, las redes, las cuentas, los servicios en la nube, la comunicación en línea, la inteligencia artificial generativa, las imágenes y grabaciones, la ciberseguridad, la protección de datos y los teléfonos móviles. También se aplica a las conductas en línea fuera del colegio cuando estén relacionadas con el centro o repercutan en la seguridad, el bienestar, la reputación o el aprendizaje de la comunidad escolar.

Esta política debe leerse junto con la Política de Salvaguarda y Protección de Menores, la Política de Comportamiento, la Política contra el Acoso Escolar, la Política de Privacidad y Protección de Datos, el Código de Conducta del Personal y el Código de la Comunidad Morna, así como con los Acuerdos de Uso Aceptable enumerados en el apartado 15. Cuando se detecte una inquietud relativa a la protección de menores, tendrán prioridad los procedimientos de protección correspondientes.

2. Principales Riesgos en Internet

El colegio procura proteger a los alumnos frente a contenidos nocivos o inapropiados, incluidos la pornografía, la violencia, los discursos de odio, el extremismo, los contenidos sobre autolesiones y la desinformación; la captación de menores, la explotación, la sextorsión y el acoso sexual en línea; el ciberacoso, la suplantación de identidad, el robo de identidad y la difusión insegura de información personal o imágenes; las imágenes de desnudos o semidesnudos, las falsificaciones ultrarrealistas (*deepfakes*) y los contenidos nocivos generados por inteligencia artificial; las estafas, el *phishing*, los ataques informáticos, el software malicioso y las cuentas comprometidas; el tiempo excesivo frente a las pantallas, los juegos de azar y los retos peligrosos en internet; el plagio, las infracciones de derechos de autor y el uso indebido de la inteligencia artificial generativa; y los intentos de eludir los controles del colegio mediante VPN, puntos de acceso personales, servidores proxy o métodos similares.

3. Funciones y Responsabilidades

El director del colegio es el responsable de esta política y de su aplicación operativa. Se asegura de que las normas de seguridad en internet se incorporen a la enseñanza, la gestión del comportamiento, las prácticas del personal y la comunicación con las familias; de que el personal reciba la formación adecuada; de que se distribuyan y revisen los Acuerdos de Uso Aceptable; y de que las infracciones graves o reiteradas se traten de manera coherente.

La directora ejecutiva ejerce la supervisión estratégica, sin sustituir la responsabilidad operativa del director del colegio respecto a la aplicación de esta política. Se asegura de que existan recursos y mecanismos de supervisión adecuados y recibe información sobre los incidentes informáticos significativos, las violaciones graves de datos, los fallos importantes de los sistemas de filtrado o supervisión y otros incidentes que supongan un riesgo considerable para el colegio.

El equipo informático tiene la responsabilidad técnica de la seguridad y el funcionamiento de las redes, cuentas y dispositivos gestionados por el colegio. Mantiene los sistemas de filtrado y supervisión, la gestión de dispositivos, los controles de acceso, las copias de seguridad y las medidas de seguridad; investiga las alertas técnicas y los incidentes informáticos; conserva las pruebas técnicas pertinentes; ayuda a contener y resolver los incidentes; y comunica las inquietudes relativas a la protección de menores o de datos a la persona responsable correspondiente.

Los responsables designados de protección de menores (DSL) se encargan de las cuestiones de protección de menores relacionadas con internet, incluidas la captación, la explotación, la sextorsión, las imágenes sexuales, las falsificaciones ultrarrealistas nocivas, el acoso, la radicalización y otros daños en línea. Los DSL deciden las medidas de protección, los registros, el contacto con los padres o tutores y las derivaciones externas de conformidad con la Política de Salvaguarda y Protección de Menores.

El personal docente y demás personal es responsable de proporcionar una supervisión adecuada, utilizar recursos digitales apropiados para la edad de los alumnos, cumplir el Código de Conducta del Personal y el Acuerdo de Uso Aceptable del Personal, proteger la información confidencial y comunicar con prontitud las inquietudes relativas a la protección de menores, cuestiones técnicas o protección de datos. El personal no debe investigar incidentes de protección de menores más allá de lo necesario para identificar y comunicar la inquietud.

Los alumnos deben utilizar la tecnología de forma segura, responsable y respetuosa; proteger las contraseñas y la información personal; cumplir el Acuerdo de Uso Aceptable del Alumnado y las normas sobre la ausencia de teléfonos móviles; y comunicar las inquietudes con prontitud.

Se espera que los **padres, madres y cuidadores** apoyen las expectativas del colegio en materia de seguridad en línea y asuman la responsabilidad de supervisar y gestionar adecuadamente el uso que sus hijos hacen de la tecnología fuera del horario escolar, tal como se establece en la sección 6. Deben recurrir a la oficina del colegio para cualquier contacto urgente durante la jornada escolar y cumplir la norma sobre teléfonos móviles dentro del perímetro vallado del colegio, tal como se establece en la sección 10.

4. Uso Seguro de la Tecnología y de los Sistemas del Colegio

El acceso a internet en el colegio deberá realizarse normalmente a través de la red autorizada. Los recursos en línea utilizados en las clases deben ser pertinentes, adecuados para la edad de los alumnos y conformes con las instrucciones del profesorado. Los usuarios no deben eludir, desactivar ni interferir con los sistemas de filtrado, supervisión, gestión de dispositivos o seguridad, incluido mediante VPN, puntos de acceso personales, servidores proxy o software no autorizado.

Los dispositivos gestionados por el colegio deben utilizarse de conformidad con las normas del centro y el Acuerdo de Uso Aceptable correspondiente. Los alumnos de Secundaria deben utilizar ordenadores portátiles aprobados y gestionados por el colegio, salvo que se autorice una excepción. Los relojes inteligentes y otros dispositivos ponibles no deben utilizarse para enviar mensajes, llamar, grabar ni acceder a internet durante la jornada escolar, salvo que exista una autorización médica u otra excepción autorizada.

La información del colegio debe crearse, almacenarse y compartirse mediante los sistemas autorizados del centro. Los usuarios no deben transferir información escolar confidencial o sensible a cuentas personales, servicios en la nube no autorizados, soportes extraíbles o aplicaciones no aprobadas.

5. Educación sobre Seguridad en Internet

Mediante la educación personal, social y para la salud (PSHE), las TIC e Informática y otras asignaturas pertinentes, los alumnos aprenderán a evaluar críticamente la información en línea; reconocer la desinformación, los sesgos y las falsificaciones ultrarrealistas; comunicarse de forma segura y respetuosa; proteger su privacidad, sus contraseñas y su reputación digital; identificar la captación, la explotación, la sextorsión, el ciberacoso y el acoso; comunicar inquietudes; utilizar imágenes, grabaciones, contenidos en línea e inteligencia artificial generativa de forma segura y legal; reconocer estafas, phishing y riesgos de ciberseguridad; y desarrollar hábitos saludables de uso de las pantallas.

El personal recibirá formación inicial y orientaciones periódicas adecuadas a sus funciones. Se proporciona formación sobre protección de datos, y los sistemas de filtrado y supervisión y la ciberseguridad se abordan mediante las medidas más amplias de protección de menores e informática del colegio. La formación actualizada sobre protección de menores a través de Tes Develop incluye inteligencia artificial, protección de menores y uso responsable, y será completada por todo el personal. La formación y las orientaciones se revisarán y actualizarán según proceda para reflejar los riesgos emergentes y las prácticas del colegio. Se facilitará a los padres y tutores información adecuada para reforzar el uso seguro de la tecnología en casa.

6. Responsabilidad de las Familias y Seguridad en Línea Fuera del Horario Escolar

Los padres, madres y cuidadores tienen la responsabilidad principal de supervisar y gestionar el uso que sus hijos hacen de los dispositivos personales, el acceso a internet, las redes sociales, los servicios de mensajería, las plataformas de videojuegos y otros servicios en línea fuera del horario escolar.

El colegio recomienda encarecidamente a los padres, madres y cuidadores que establezcan límites adecuados a la edad de sus hijos en relación con el tiempo de pantalla, las aplicaciones, las redes sociales, la comunicación en línea y el acceso a contenidos en internet, y que utilicen de forma adecuada los controles parentales y las herramientas de filtrado.

Para apoyar a las familias, Morna International College facilita el acceso a Qustodio para los dispositivos de los alumnos gestionados por el colegio. Fuera del horario escolar, los padres, madres y cuidadores pueden utilizar Qustodio para gestionar los controles y filtros adecuados en el dispositivo gestionado por el colegio. Actualmente, el colegio también ofrece a las familias la posibilidad de proteger un dispositivo personal adicional por alumno. Las instrucciones de registro y configuración se incluyen en el Anexo 1 — Guía rápida de Qustodio para familias.

7. Inteligencia Artificial Generativa

La inteligencia artificial solo podrá utilizarse cuando sea adecuada para la tarea de aprendizaje y conforme a las instrucciones del profesor. Los alumnos no deben presentar trabajos generados por inteligencia artificial como propios ni utilizarla para eludir los requisitos de evaluación. Deberán declarar su uso cuando se exija. La información escolar confidencial, sensible o personal no debe introducirse en sistemas de inteligencia artificial no aprobados, y la información generada por estos sistemas debe comprobarse de forma crítica.

La inteligencia artificial nunca debe utilizarse para crear contenido abusivo, engañoso, discriminatorio, sexualizado o nocivo. Las falsificaciones ultrarrealistas o imágenes manipuladas que sean perjudiciales se tratarán como una falta grave y, cuando proceda, como un asunto de protección de menores. Cualquier sospecha de imágenes perjudiciales generadas por inteligencia artificial que involucren a un alumno debe tratarse conforme al procedimiento sobre imágenes perjudiciales del apartado 12.

8. Cuentas, Ciberseguridad y Dispositivos Perdidos

Las contraseñas deben mantenerse confidenciales y los usuarios no deben acceder a la cuenta de otra persona. Debe utilizarse la autenticación multifactor cuando se exija. Las sospechas de phishing, software malicioso, cuentas comprometidas o accesos no autorizados deben comunicarse inmediatamente al equipo informático. El usuario debe dejar de interactuar con el mensaje o sistema sospechoso y seguir las instrucciones del equipo informático; cuando se le indique, deberá cambiar las contraseñas sin demora.

La pérdida o el robo de cualquier dispositivo gestionado por el colegio, o de un dispositivo personal autorizado para almacenar información escolar o acceder a ella, debe comunicarse inmediatamente al equipo informático y al superior directo del usuario o al profesor correspondiente. La comunicación debe indicar cuándo y dónde se vio por última vez el dispositivo y si puede contener información personal o confidencial, o permitir el acceso a ella. Cuando dicha información pueda ser accesible, el incidente también debe tratarse como una posible violación de datos conforme al apartado 9. El equipo informático adoptará medidas proporcionadas, que podrán incluir la suspensión de cuentas, el restablecimiento de contraseñas, el bloqueo o borrado remoto cuando sea técnicamente posible, la conservación de los registros técnicos pertinentes y la evaluación de si se requieren otras medidas de seguridad o protección de datos.

En caso de un incidente informático significativo, el equipo informático dirigirá las medidas técnicas de contención, conservación de pruebas, recuperación y seguridad; el director del colegio coordinará las decisiones educativas y operativas; los DSL dirigirán cualquier respuesta de protección de menores; y se informará a la directora ejecutiva cuando el incidente sea grave o afecte de manera significativa al funcionamiento, los datos o la reputación del colegio. Los usuarios no deben realizar su propia investigación técnica, eliminar pruebas ni comunicar información sobre el incidente al exterior, salvo que estén autorizados.

9. Protección de Datos y Posibles Violaciones de Datos

Los datos personales deben tratarse conforme a la Política de Privacidad y Protección de Datos. La información sensible solo debe compartirse cuando sea necesario, mediante sistemas autorizados y con destinatarios autorizados. La información personal o las imágenes no deben publicarse sin el permiso correspondiente u otra base jurídica válida.

Una posible violación de datos incluye la pérdida de información, su divulgación accidental, un correo electrónico enviado al destinatario equivocado, un acceso no autorizado, credenciales comprometidas, la pérdida de un dispositivo que contenga datos personales o cualquier otro incidente que pueda afectar a la confidencialidad, integridad o disponibilidad de los datos personales. El personal debe comunicar inmediatamente cualquier posible violación a la persona responsable de Finanzas y Apoyo Administrativo, encargada de la gestión diaria de los asuntos de protección de datos. También se debe informar al director del colegio cuando el incidente afecte a cuestiones operativas o educativas, y al equipo informático cuando estén implicados sistemas técnicos o cuentas.

La persona responsable de Finanzas y Apoyo Administrativo garantizará que el incidente se registre, contenga y evalúe conforme a la Política de Privacidad y Protección de Datos, incluida cualquier notificación o comunicación necesaria a la directora ejecutiva, en calidad de representante legal del colegio. El personal no debe ocultar una posible violación, investigarla por su cuenta ni contactar con las personas afectadas salvo que reciba instrucciones para hacerlo.

10. Colegio sin Teléfonos Móviles y Normas en el Recinto Escolar

Morna International College es un colegio sin teléfonos móviles para todos los alumnos, incluidos los de Years 12 y 13. Los alumnos no pueden utilizar teléfonos móviles dentro del perímetro vallado del colegio durante la jornada escolar, salvo que se haya autorizado una excepción específica. Esto se aplica durante las clases, el registro de asistencia, los descansos, el almuerzo y los desplazamientos entre clases. Los padres y tutores deben contactar con los alumnos a través de la Secretaría; los alumnos que necesiten contactar con casa deben pedir ayuda al personal.

Se espera que el personal, los padres, los tutores y los visitantes mantengan sus teléfonos móviles personales fuera de la vista y no los utilicen dentro del perímetro vallado del colegio durante el horario escolar, salvo cuando sea necesario por una emergencia, una necesidad médica acordada, un fin autorizado de protección de menores u operativo, u otra circunstancia necesaria aprobada por el colegio. El uso de dispositivos personales por parte del personal también debe cumplir el Código de Conducta del Personal, el Acuerdo de Uso Aceptable del Personal y el apartado 11 de esta política.

Los padres y tutores también deben consultar el Código de la Comunidad para Padres y Tutores para conocer más detalles sobre las normas del colegio.

El uso no autorizado de un teléfono móvil, reloj inteligente u otro dispositivo electrónico personal por parte de un alumno normalmente dará lugar a su confiscación, como mínimo, hasta el final de la jornada escolar, salvo por motivos de protección del menor, médicos, relacionados con una discapacidad u otras circunstancias excepcionales. El dispositivo confiscado se entregará sin demora al responsable de la etapa correspondiente o al director del colegio, se registrará y se guardará de forma segura en una oficina cerrada con llave. El colegio cuidará razonablemente los dispositivos confiscados, pero no se responsabiliza de los daños preexistentes ni de las pérdidas derivadas del incumplimiento del procedimiento de entrega por parte del alumno.

En caso de una primera infracción o de una infracción leve, el dispositivo normalmente se devolverá al alumno al final de la jornada escolar. En caso de infracciones reiteradas, el colegio podrá retener el dispositivo durante más tiempo y exigir que lo recoja un padre, madre, cuidador u otro adulto autorizado. El colegio notificará al padre, madre o cuidador cuando se vaya a retener un dispositivo más allá del final de la jornada escolar y le informará de las condiciones de recogida.

Las infracciones reiteradas, ocultadas deliberadamente o cometidas desafiando las normas podrán dar lugar a otras sanciones conforme a la Política de Comportamiento. El uso indebido que implique grabaciones, acoso escolar, acoso, amenazas, contenido sexual o perjudicial, o pruebas relevantes para la protección de menores se remitirá a un DSL y podrá dar lugar a que el dispositivo se retenga o se gestione de otro modo cuando sea necesario para proteger a un menor o conservar pruebas. El personal no debe examinar el contenido de un teléfono confiscado salvo que esté específicamente autorizado y que los procedimientos aplicables del colegio lo permitan. Las exenciones por motivos médicos, relacionados con una discapacidad u otras circunstancias excepcionales deben acordarse previamente y quedar registradas.

11. Uso de Dispositivos Personales por Parte del Personal

Siempre que se faciliten, el personal deberá utilizar los dispositivos gestionados por el colegio y los sistemas escolares autorizados para los asuntos del centro. Los dispositivos personales no deben utilizarse para fotografiar, filmar o grabar a los alumnos, acceder a información confidencial sobre ellos o almacenarla, ni llevar a cabo comunicaciones escolares habituales, salvo que exista un procedimiento escolar expresamente autorizado que lo permita.

Cuando se autorice excepcionalmente el uso de un dispositivo personal para una finalidad escolar necesaria, deberá utilizarse la cantidad mínima de información, transferirse al sistema escolar autorizado tan pronto como sea viable y eliminarse después de forma segura cualquier copia local. No deben utilizarse cuentas personales de mensajería ni de redes sociales para comunicarse en privado con los alumnos. Todo uso por parte del personal sigue sujeto al Código de Conducta del Personal, la Política de Privacidad y Protección de Datos y el Acuerdo de Uso Aceptable del Personal.

12. Imágenes, Grabaciones e Imágenes Perjudiciales

Los alumnos no deben fotografiar, filmar ni grabar a otras personas, clases, reuniones o conversaciones sin autorización. Las imágenes y grabaciones educativas solo deben captarse, almacenarse y compartirse mediante los procedimientos autorizados, y su publicación externa requiere la autorización correspondiente.

Cualquier inquietud relacionada con imágenes de un alumno desnudo o semidesnudo, falsificaciones ultrarrealistas de carácter sexual, difusión coactiva de imágenes, sextorsión o imágenes potencialmente ilegales debe comunicarse inmediatamente a un DSL. El personal y los alumnos no deben pedir que se les envíe la imagen, reenviarla o copiarla, ni visualizarla, guardarla, imprimirla o hacer una captura de pantalla sin necesidad. El DSL seguirá el procedimiento de protección de menores del colegio, registrará las decisiones, valorará el contacto con los padres o tutores y la derivación externa, y garantizará que cualquier prueba se conserve únicamente de forma segura y proporcionada.

Cuando una imagen o grabación también constituya prueba de acoso escolar, acoso, amenazas u otro incidente de comportamiento, la respuesta de protección de menores tendrá prioridad si existe riesgo de daño. Las decisiones sobre la confiscación de un dispositivo o el acceso a él deben tomarse en consulta con un DSL cuando pueda contener imágenes perjudiciales.

13. Alertas de Filtrado y Supervisión

El colegio utiliza sistemas de filtrado y supervisión como parte de sus controles de protección de menores y ciberseguridad. El equipo informático es responsable de mantener los sistemas técnicos. Las alertas son revisadas por el personal de soporte informático y los responsables de atención pastoral pertinentes, según la naturaleza de cada alerta. Los sistemas de filtrado y supervisión no sustituyen la supervisión del personal.

Las alertas que indiquen un posible riesgo de protección de menores, contenido perjudicial, intentos de eludir los controles, cuentas comprometidas o actividad inusual deben revisarse con prontitud según su gravedad. El personal de soporte informático abordará los problemas técnicos y conservará los registros pertinentes cuando proceda. Cuando una alerta pueda indicar un riesgo para un menor, debe remitirse sin demora a un DSL o al responsable de protección correspondiente, de acuerdo con los procedimientos del colegio. Los intentos reiterados o deliberados de eludir los controles también deben comunicarse al director del colegio o al responsable pertinente de atención pastoral o comportamiento.

Las actuaciones y los resultados derivados de las alertas se registrarán mediante el procedimiento informático, pastoral o de protección de menores correspondiente, según la naturaleza de la inquietud. El personal que revise las alertas debe evitar el acceso innecesario a material perjudicial y no debe copiarlo ni difundirlo, salvo cuando lo exija específicamente un procedimiento técnico o de protección autorizado.

14. Comunicación, Registro y Respuesta ante Incidentes

Las inquietudes relativas a la protección de menores deben comunicarse inmediatamente a un DSL. Las cuestiones de ciberseguridad deben comunicarse con prontitud al equipo informático. Las posibles violaciones de datos deben comunicarse por la vía establecida en el apartado 9. Cuando un incidente pertenezca a más de una categoría, los responsables correspondientes deben coordinar su respuesta en lugar de tratar cada aspecto de forma aislada.

Las inquietudes y las actuaciones deben registrarse de forma objetiva, incluyendo qué se comunicó, quién lo hizo, cuándo ocurrió, qué medidas inmediatas se adoptaron y a quién se remitió el asunto. Las posibles pruebas deben conservarse sin visualizar, copiar ni reenviar innecesariamente contenido perjudicial. Normalmente, se informará a los padres o tutores cuando proceda, salvo que hacerlo pueda aumentar el riesgo, perjudicar una investigación o contradecir las indicaciones de protección de menores.

El colegio podrá remitir asuntos a organismos externos, proveedores de servicios, autoridades reguladoras o la policía cuando sea necesario. Los incidentes graves se revisarán posteriormente para mejorar los controles técnicos, la educación, los procedimientos o la formación.

15. Acuerdos de Uso Aceptable y Políticas Relacionadas

La Política de Uso Aceptable del colegio y los acuerdos asociados forman parte de su marco de seguridad en internet y establecen las normas para el uso adecuado de los sistemas informáticos, las redes y los dispositivos del colegio por parte de alumnos y personal. Cualquier acuerdo independiente sobre dispositivos o redes gestionados por el colegio que este adopte debe leerse junto con estas disposiciones. El director del colegio es responsable de garantizar que los acuerdos de uso aceptable vigentes puedan identificarse, estén disponibles y se revisen anualmente junto con esta política.

Se espera que los alumnos y el personal cumplan los acuerdos de uso aceptable que les correspondan. Cuando se emita una confirmación o un acuerdo independiente, deberá completarse en el momento que determine el colegio, normalmente al incorporarse, al recibir un dispositivo gestionado por el centro o después de una modificación importante. Se debe informar a los padres y tutores de las normas aplicables a los alumnos y de cualquier confirmación o consentimiento requerido.

Las políticas, códigos y guías relacionados son: Política de Salvaguarda y Protección de Menores; Política de Comportamiento; Política de Privacidad y Protección de Datos; Política contra el Acoso Escolar; Código de Conducta del Personal; Código de la Comunidad para Padres, Madres y Cuidadores; y Anexo 1 — Guía rápida de Custodio para familias.

Las medidas operativas relativas a la confiscación de teléfonos móviles, las alertas de filtrado y supervisión, los incidentes de ciberseguridad y dispositivos perdidos, las violaciones de datos y las imágenes perjudiciales o sexuales se abordan mediante la Política de Salvaguarda y Protección de Menores, la Política de Comportamiento, los acuerdos de uso aceptable, la Política de Privacidad y Protección de Datos y los procesos informáticos pertinentes del colegio. Estas medidas no tienen necesariamente la forma de procedimientos independientes. El personal debe seguir la política pertinente y el proceso establecido de protección de menores, atención pastoral, informática o protección de datos según la naturaleza del incidente.

16. Revisión y Cumplimiento

El director del colegio revisará esta política anualmente o antes si se produce un incidente significativo o un cambio importante en la tecnología, las orientaciones de protección de menores o los sistemas escolares. La revisión incluirá aportaciones del equipo informático y los DSL, y tendrá en cuenta los sistemas de filtrado y supervisión, los patrones de incidentes, la formación del personal, los Acuerdos de Uso Aceptable y la eficacia de los procedimientos que mantienen el colegio libre de teléfonos móviles.

El incumplimiento de esta política podrá dar lugar a medidas conforme a la Política de Comportamiento, el Código de Conducta del Personal, los procedimientos contractuales o disciplinarios, los procedimientos de protección de menores u otros procesos pertinentes del colegio, según la persona implicada y la gravedad del asunto.

Control de la Política

Título de la política	Política de Seguridad en Internet y Dispositivos Electrónicos 2026/2027
Responsable de la política	Director del colegio
Responsable de su aplicación	Director del colegio y Equipo Directivo
Dirigida a	Toda la comunidad escolar
Aprobada por	Directora ejecutiva
Fecha de aprobación	30 de septiembre de 2026
Frecuencia de revisión	Al menos una vez al año y antes si se produce un cambio legal, reglamentario o procedimental
Próxima fecha de revisión	30 de septiembre de 2027
Versión	1.0

ANEXO 1 - GUÍA RÁPIDA DE QUSTODIO PARA FAMILIAS

Controles parentales para los dispositivos de los alumnos gestionados por el colegio fuera del horario escolar

1. Cree su cuenta

Acceda a **qustodio.com/my-school** y regístrese con la dirección de correo electrónico personal que tenga registrada en el colegio. Es posible que se le solicite el año de nacimiento de su hijo.

2. Abra el perfil de su hijo

Seleccione a su hijo en el panel de control familiar para consultar su actividad y configurar las reglas disponibles.

3. Configure los controles parentales

Seleccione los controles que se adapten a su familia, incluidos **el filtrado web, el bloqueo de aplicaciones, las alertas de contenido, los límites de tiempo de pantalla y los horarios de descanso o rutinas.**

4. Horario escolar

Durante el horario escolar, el colegio gestiona el dispositivo escolar. **El control parental estará disponible cuando finalice la jornada escolar.**

5. Dispositivo adicional

Actualmente, el servicio ofrecido por el colegio incluye **la protección del portátil escolar fuera del horario escolar y de un dispositivo personal adicional por alumno.**

6. Vuelva a acceder a Qustodio

Tras registrarse, acceda al panel de control parental en **family.qustodio.com/parents-app**. No es necesario instalar nada en el dispositivo del alumno gestionado por el colegio.

Importante: Qustodio se proporciona para apoyar a las familias. Los padres, madres y cuidadores siguen siendo responsables de supervisar y gestionar el uso que sus hijos hacen de la tecnología fuera del horario escolar.