GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES
ACCIÓN EDUCATIVA EXTERIOR
INSTITUTO ESPAÑOL VICENTE CAÑADA BLANCH

Growing together to achieve international success

POLÍTICA DE SEGURIDAD ELECTRÓNICA

incluido EYFS

Se trata de una política para toda la escuela

Revisado: Febrero 2024

Próxima revisión: Enero 2026

317 Portobello Road
Londres W10 5SZ
Teléfono: 020 8969 2664
canada.blanch.uk@educacion.gob.es
http://vicentecanadablanch.educacion.es/

1. Objetivos

Esta política tiene por objeto:

- Establecer las expectativas de comportamiento, actitudes y actividades en línea de todos los miembros de la comunidad y el uso de la tecnología digital en IE Vicente Cañada Blanch.
- Ayudar a todas las partes interesadas a reconocer que las normas de comportamiento en línea/digital (incluida la actividad en las redes sociales) deben mantenerse más allá de los confines de la escuela y de la jornada escolar, e independientemente del dispositivo o la plataforma.
- Facilitar el uso seguro, responsable y respetuoso de la tecnología para apoyar la enseñanza y el aprendizaje, aumentar los logros y preparar a los estudiantes para los riesgos y oportunidades del mundo digital de hoy y de mañana, para sobrevivir y prosperar en línea.
- Ayudar al personal escolar que trabaja con niños a comprender sus funciones y responsabilidades para trabajar de forma segura y responsable con la tecnología y el mundo en línea:
    - para la protección y el beneficio del alumnado a su cargo.
    - para su propia protección, evitar acusaciones erróneas o malintencionadas y comprender mejor sus propias normas y prácticas.
    - en beneficio de la escuela, apoyando la ética, las metas y los objetivos de la escuela, y protegiendo la reputación de la escuela y de la profesión.
- Establecer estructuras claras por las que se tratarán las faltas en línea y los procedimientos a seguir en caso de dudas o preocupaciones, con referencia a otras políticas escolares como el Código de Conducta o la Política Antiacoso.

2. Alcance

Esta política se aplica a todos los miembros de la comunidad IE Vicente Cañada Blanch (incluido el personal, voluntarios, contratistas, estudiantes / alumnado, familias / cuidadores, visitantes y usuarios de la comunidad) que tienen acceso a nuestra tecnología digital, redes y sistemas, ya sea en el sitio o de forma remota, y en cualquier momento. Incluye la Educación Infantil.

3. Funciones y responsabilidades

El I.E.Vicente Cañada Blanch es una comunidad y todos sus miembros tienen el deber de comportarse respetuosamente en línea y fuera de línea, de utilizar la tecnología para la enseñanza y el aprendizaje y para prepararse para la vida después de la escuela, y de informar inmediatamente de cualquier preocupación o comportamiento inapropiado, para proteger al personal, alumnado, las familias y la reputación de la escuela.

Director - Antonio Simón Saiz

Responsabilidades clave:

- Fomentar una cultura de salvaguardia en la que la seguridad en línea esté plenamente integrada en la salvaguardia de toda la escuela.
- Supervisar las actividades del *Designated Safeguarding Lead* y asegurarse de que se cumplen y apoyan plenamente las responsabilidades del DSL enumeradas en la sección siguiente.
- Garantizar el cumplimiento de las políticas y procedimientos por parte de todo el personal.
- Recibir formación sobre protección en línea y fuera de línea, de conformidad con las directrices legales y las orientaciones pertinentes de los Servicios Sociales.
- Estar en contacto con el *Designated Safeguarding Lead* para todas las cuestiones de seguridad en línea que puedan surgir y recibir actualizaciones periódicas sobre cuestiones escolares e información más amplia sobre políticas y prácticas.
- Asumir la responsabilidad general de la gestión de los datos y la seguridad de la información, garantizando que la oferta de la escuela sigue las mejores prácticas en el tratamiento de la información, ayudando a garantizar que la protección de los niños es siempre lo primero y que los procesos de protección de datos apoyan el intercambio cuidadoso y legal de información.
- Garantizar que la escuela implementa y hace un uso efectivo de los sistemas y servicios TIC apropiados, incluidos el filtrado y la supervisión seguros para la escuela, los sistemas de correo electrónico protegidos y que toda la tecnología, incluidos los sistemas en la nube, se implementan de acuerdo con los principios de seguridad infantil.
- Responsabilizarse de que todo el personal reciba la formación adecuada para desempeñar sus funciones de salvaguardia y seguridad en línea.
- Comprender y sensibilizar a todo el personal sobre los procedimientos que deben seguirse en caso de incidente grave de protección en línea.
- Garantizar que se llevan a cabo evaluaciones de riesgo adecuadas para que el plan de estudios satisfaga las necesidades del alumnado, incluido el riesgo de que los niños se radicalicen.
- Garantizar que existe un sistema para supervisar y apoyar al equipo TIC que lleva a cabo los procedimientos técnicos internos de seguridad en línea.

Designated Safeguarding Lead - Mario Muñoz Checa

Responsabilidades clave:

El *Designated Safeguarding Lead* asume la responsabilidad principal en materia de salvaguardia y protección de la infancia, incluida la seguridad en línea.

- Garantizar una revisión periódica y una comunicación abierta entre la escuela y el equipo TIC.
- Garantizar un enfoque eficaz de la seguridad en línea que faculte a la escuela para proteger y educar a la comunidad en su uso de la tecnología y establezca mecanismos para identificar, intervenir y escalar cualquier incidente cuando proceda.
- Estar en contacto con la autoridad local y colaborar con otros organismos de acuerdo con la iniciativa "*Working Together to Safeguard Children*".
- Asumir la responsabilidad cotidiana de las cuestiones de seguridad en línea y ser consciente de la posibilidad de que surjan problemas graves de protección de menores.
- Trabajar con el director de la escuela para garantizar que la protección de la infancia sea siempre lo primero y que los procesos de protección de datos apoyen el intercambio cuidadoso y legal de información.
- Manténgase al día de las últimas tendencias en seguridad en línea.
- Revisar y actualizar esta política, otros documentos sobre seguridad en línea y la estrategia en la que se basan, en armonía con las políticas de comportamiento, salvaguardia, prevención y otras, y presentarlos para su revisión a los propietarios/fideicomisarios.
- Recibir actualizaciones periódicas sobre temas de seguridad en línea y legislación, y estar al tanto de las tendencias locales y escolares.
- Garantizar que la educación en materia de seguridad en línea se integre en el plan de estudios y, más allá, en la vida escolar en general.
- Promover la concienciación y el compromiso con la seguridad en línea en toda la comunidad escolar, con especial atención a las familias, que a menudo agradecen el apoyo escolar en este ámbito, pero también incluyendo a las familias de difícil acceso.
- Colaborar con el personal técnico y de apoyo de la escuela, según proceda.
- Comunicarse regularmente con el SLT y el equipo TIC designado para discutir los problemas actuales, revisar los registros de incidentes y los registros de filtrado/control de cambios y discutir el filtrado y la supervisión.
- Garantizar que todo el personal conozca los procedimientos que deben seguirse en caso de incidente de seguridad en línea, y que éstos se registren de la misma manera que cualquier otro incidente de protección.
- Garantizar que las orientaciones del Departamento de Educación de 2018 sobre la violencia sexual y el acoso se sigue en toda la escuela y que el personal adopta un enfoque de tolerancia cero a esto, así como a la intimidación.

- Facilitar formación y asesoramiento a todo el personal:
  - todo el personal debe leer KCSIE Parte 1 y todos los que trabajan con niños el Anexo A.
  - transmitir en cascada el conocimiento de los riesgos y oportunidades a toda la organización

Todo el personal

Responsabilidades clave:

- Entender que la seguridad en línea es una parte fundamental de la protección; como tal, forma parte del trabajo de todos: nunca pienses que otra persona se encargará de ello.
- Saber que el *Designated Safeguarding Lead* (DSL) es Mario Muñoz Checa, el Responsable de TIC es Paul Flores y el Coordinador de TIC es Cristóbal Alonso.
- Leer la Parte 1, Anexo A de KCSIE.
- Leer y siga esta política junto con la política principal de salvaguardia de la escuela (Anexo 2).
- Registrar los incidentes de seguridad en línea de la misma manera que cualquier incidente de protección e informe de acuerdo con los procedimientos de la escuela.
- Comprender que la protección es a menudo un rompecabezas, así que no se guarde nada para sí mismo.
- Firmar y respetar la política de seguridad electrónica de la escuela y seguir el Código de Conducta.
- Notificar al equipo DSL/TIC si la política no refleja la práctica en su centro escolar y siga los procedimientos de escalada si no se actúa con prontitud ante las preocupaciones.
- Identificar oportunidades para encauzar la seguridad en línea a través de todas las actividades escolares, tanto fuera del aula como dentro del plan de estudios, apoyando a los responsables del plan de estudios/etapas/asignaturas y aprovechando al máximo las oportunidades de aprendizaje inesperadas que surjan.
- Siempre que supervise el uso de la tecnología en la escuela o en tareas escolares, fomentar un uso sensato, controlar lo que hace el alumnado y tener en cuenta los posibles peligros y la adecuación a la edad de los sitios web.
- Supervisar y guiar cuidadosamente al alumnado cuando participen en actividades de aprendizaje que impliquen el uso de tecnología en línea (incluidas las actividades extraescolares y de ampliación del horario escolar, si procede), ayudándoles con las habilidades de búsqueda, el pensamiento crítico, los materiales apropiados para su edad y la señalización, así como con cuestiones jurídicas como los derechos de autor y la legislación sobre datos.
- Animar al alumnado/estudiantes a seguir su política de uso aceptable, recuérdesela y aplique las sanciones escolares.

- Notificar al equipo DSL/TIC las nuevas tendencias y problemas antes de que se conviertan en un problema.
- Adoptar un planteamiento de tolerancia cero frente a la intimidación y el acoso sexual de bajo nivel.
- Tener en cuenta que es más probable ver o escuchar problemas de seguridad en línea en el patio, los pasillos y otras zonas comunes fuera del aula.
- Modelar comportamientos seguros, responsables y profesionales en su propio uso de la tecnología.
- Comprender las expectativas, funciones y responsabilidades aplicables en relación con el filtrado y la supervisión.

Director de informática: Cristóbal Alonso

Técnico informático: Paul Flores

Responsabilidades clave:

- Como se indica en la sección "todo el personal", además:
- Mantenerse al día de la política de seguridad en línea de la escuela y de la información técnica para desempeñar eficazmente su función de seguridad en línea e informar y poner al día a los demás según proceda.
- Colaborar estrechamente con el *Designated Safeguarding Lead* y el equipo de TIC para garantizar que los sistemas y redes escolares reflejen la política del centro.
- Garantizar que las partes interesadas antes mencionadas comprendan las consecuencias de los servicios existentes y de cualquier cambio en estos sistemas, especialmente en términos de acceso a registros/datos personales y sensibles y a sistemas como el modo YouTube, los ajustes de filtrado web, los permisos para compartir archivos en plataformas en la nube, etc.
- Apoyar y asesorar sobre la aplicación de un filtrado y una supervisión adecuados, según lo decidido por el DSL, el equipo TIC y el SLT.
- Mantener actualizados los dispositivos de seguridad en línea de la escuela.
- Informar de los problemas relacionados con la seguridad en línea de los que tengan conocimiento, de acuerdo con la política del centro.

Voluntarios y contratistas

Responsabilidades clave:

- Leer y comprender esta política.
- Informar de cualquier preocupación, por pequeña que sea, al *Designated Safeguarding Lead* / Equipo TIC.

- Estar al corriente de las cuestiones y orientaciones actuales sobre seguridad en línea.
- Modelar comportamientos seguros, responsables y profesionales en su propio uso de la tecnología.

Alumnado

Responsabilidades clave:

- Comprender la importancia de denunciar los abusos, el uso indebido o el acceso a materiales inapropiados.
- Saber qué hacer si ellos o alguien que conocen se sienten preocupados o vulnerables al utilizar la tecnología en línea.
- Comprender la importancia de adoptar comportamientos seguros y responsables y buenas prácticas de seguridad en línea cuando se utilizan tecnologías digitales fuera de la escuela y darse cuenta de que las políticas de uso aceptable de la escuela cubren las acciones fuera de la escuela, incluidas las redes sociales.
- Comprender las ventajas/oportunidades y los riesgos/peligros del mundo en línea y saber con quién hablar en la escuela o fuera de ella si surgen problemas.

El alumnado dirigirá cualquier preocupación que puedan tener sobre la seguridad en línea a su profesorado o directamente al *Designated Safeguarding Lead*. También pueden hacer uso del Buzón de Salvaguardia.

Familias/cuidadores

Responsabilidades clave:

- Leer y comprender esta política y animar a sus hijos a seguirla.
- Consultar con la escuela si tienen alguna duda sobre el uso que sus hijos hacen de la tecnología.
- Promover una seguridad en línea positiva y modelar comportamientos seguros, responsables y positivos en su propio uso de la tecnología, incluidas las redes sociales: no compartir imágenes o datos de otras personas sin permiso y abstenerse de publicar comentarios negativos, amenazadores o violentos sobre otras personas, incluidos el personal del centro, los voluntarios, los propietarios, los contratistas, el alumnado u otras familias/cuidadores.

4. Gestión de problemas e incidentes de seguridad en línea

Los problemas de seguridad en línea deben tratarse de la misma manera que cualquier otro problema de protección, por lo que todos los profesionales **deberían** hablar con el *Designated Safeguarding Lead* para contribuir al panorama general o poner de relieve lo que aún podría no ser un problema.

El personal no docente tendrá a menudo una visión y una oportunidad únicas de enterarse de los problemas que surgen en el patio, los pasillos y otras zonas comunes fuera de las aulas (sobre todo en relación con la intimidación y el acoso y la violencia sexuales).

Los procedimientos escolares en materia de seguridad en línea se detallan en su mayor parte en las siguientes políticas:

- Política de salvaguardia y protección de la infancia
- Política antiacoso
- Código de conducta

I.E. Vicente Cañada Blanch se compromete a tomar todas las precauciones razonables para garantizar la seguridad en línea, pero reconoce que los incidentes pueden ocurrir tanto dentro como fuera de la escuela y que los de fuera de la escuela seguirá afectando al alumnado cuando vienen a la escuela. Se anima a todos los miembros de la escuela a informar de los problemas rápidamente para que podamos tratarlos con rapidez y sensibilidad a través de los procesos de escalada de la escuela.

Cualquier sospecha de riesgo o infracción en línea debe ser comunicada al Equipo TIC / *Designated Safeguarding Lead* el mismo día.

Cualquier preocupación/alegación sobre el mal uso del personal se remite siempre directamente al Director, a menos que la preocupación sea sobre el Director, en cuyo caso la queja se remite a la Consejería de Educación y al LADO (Local Authority Designated Officer).

5. Acoso escolar

El acoso en línea debe tratarse como cualquier otra forma de acoso y debe seguirse la política de acoso escolar para el acoso en línea, que también puede denominarse ciberacoso.

Consulta en la web del IE Vicente Cañada Blanch la política Anti-bullying para más información.

6. Violencia y acoso sexual

Cualquier incidente de acoso o violencia sexual (en línea o fuera de línea) debe comunicarse al DSL, que seguirá todas las directrices. El personal debe esforzarse por fomentar una cultura de tolerancia cero. El centro escolar se toma en serio todas las formas de acoso y violencia sexual, explica que existe un continuo y que los comportamientos considerados incorrectamente de "bajo nivel" se tratan con seriedad y no se permite que se perpetúen.

7. Uso indebido de la tecnología escolar (dispositivos, sistemas, redes o plataformas).

Unas normas y procedimientos claros y bien comunicados son esenciales para regular el uso por parte de alumnado y adultos de las redes, conexiones, conectividad a Internet y dispositivos escolares, plataformas en la nube y medios sociales.

En caso de que el alumnado infrinja estas normas, se aplicarán las Normas de Convivencia del centro. Además de estas medidas, el centro se reserva el derecho a retirar, temporal o permanentemente, el acceso a la tecnología o el derecho a introducir dispositivos en las instalaciones del centro.

8. Protección y seguridad de los datos

El director y el DSL trabajan juntos para garantizar la aplicación en el Reino Unido del Reglamento General de Protección de Datos, o GDPR para el almacenamiento de datos, que garantiza que la protección de los niños sea siempre lo primero y que los procesos de protección de datos apoyen el intercambio cuidadoso y legal de información. (Anexo 1)

Se recuerda al personal que todos los datos de salvaguardia son muy sensibles y deben tratarse con la más estricta confidencialidad en todo momento, y que sólo deben compartirse a través de canales aprobados con colegas u organismos que dispongan de los permisos adecuados.

9. Filtrado y control adecuados

Keeping Children Safe in Education 2023 obliga a las escuelas a garantizar la existencia de filtros adecuados y sistemas de supervisión apropiados y a no permitir el acceso a material nocivo o inapropiado, así como a enseñar a los niños lo relativo a la enseñanza en línea y la salvaguardia.

En el I.E. Vicente Cañada Blanch, la conexión a Internet se proporciona sólo para el profesorado. Esto significa que tenemos una conexión dedicada y segura, segura para la escuela, que está protegida con cortafuegos y seguridad, incluyendo un sistema de filtrado web, que está hecho específicamente para proteger a los niños en las escuelas. Todos nuestros ordenadores tienen un programa de protección contra la congelación que restaura todos los ajustes a la configuración original después de apagar el ordenador.

Smoothwall Ltd. proporciona el sistema de filtrado y supervisión del centro. El DSL y el responsable de TIC tienen acceso al portal Smoothwall, donde se ejecutarán informes al menos una vez al año para comprobar que las medidas adecuadas para evitar que el alumnado acceda a contenidos inapropiados están actualizadas.

Cada vez que un alumno utilice un dispositivo escolar, será supervisado. Si intentan acceder a contenidos inapropiados, se enviará una alerta a las direcciones de correo electrónico del equipo de protección y del responsable de TIC.

10. Comunicaciones electrónicas

Por favor, lea esta sección junto con las referencias a las comunicaciones entre alumnado y personal en el Código de Conducta de la escuela (dentro del Manual del Personal). Esta sección sólo cubre las comunicaciones electrónicas, pero se aplican los mismos principios de transparencia, conducta adecuada y pista de auditoría.

11. Página web de la escuela

El sitio web de la escuela es un portal de información clave para la comunidad escolar, con un valor clave para su reputación. El director ha delegado la responsabilidad diaria de actualizar el contenido del sitio web en el coordinador de TIC y en el tesorero del centro.

12. Imágenes y vídeo digitales

Cuando un alumno/estudiante se incorpora a la escuela, se pregunta a las familias/tutores si dan su consentimiento para que la imagen de su hijo sea captada en fotografías o vídeos y con qué finalidad, según el Anexo I.

Todo el personal se rige por su contrato de trabajo en IE Vicente Cañada Blanch. Los miembros del personal pueden utilizar ocasionalmente teléfonos personales para capturar fotos o videos del alumnado, pero estos serán apropiados, vinculados a las actividades escolares, tomados sin secreto y no en una situación de uno a uno, y siempre se trasladarán al almacenamiento de la escuela tan pronto como sea posible, después de lo cual se eliminarán de los dispositivos personales o servicios en la nube.

Animamos a los jóvenes a pensar en su reputación en línea y en su huella digital, por lo que debemos ser buenos modelos adultos no compartiendo más de la cuenta. En su programa de educación sobre seguridad en línea, el alumnado aprende a manipular las imágenes y a considerar cómo publicarlas para una amplia gama de audiencias. Se aconseja al alumnado que tengan mucho cuidado a la hora de publicar fotos personales en las redes sociales. Se les enseña a comprender la necesidad de mantener la configuración de privacidad para no hacer pública información personal.

Se enseña al alumnado que no deben publicar imágenes o vídeos de otras personas sin su permiso. Les enseñamos los riesgos asociados al suministro de información con imágenes (incluido el nombre del archivo), que revelan la identidad de otros y su ubicación. Les enseñamos la necesidad de mantener sus datos seguros y qué hacer si son objeto de acoso o abuso.

13. Redes sociales

SM presencia del IE Vicente Cañada Blanch

El IE Vicente Cañada parte del principio de que, si nosotros no gestionamos nuestra reputación en las redes sociales, lo harán otros. En consecuencia, gestionamos y supervisamos cuidadosamente nuestra huella en las redes sociales para saber qué se dice de la escuela y responder a las críticas y los elogios de manera justa y responsable.

Los coordinadores de TIC son responsables de la gestión de nuestro sitio escolar y Twitter. Seguirán las directrices del documento de gestión de la reputación en línea de LGfL / Safer Internet Centre.

Presencia de SM en el personal, el alumnado y las familias

Las redes sociales (incluyendo aquí todas las aplicaciones, sitios y juegos que permiten compartir e interactuar entre usuarios) son un hecho de la vida moderna y, como colegio, aceptamos que muchas familias, personal y alumnado las utilicen. Esperamos que todos se comporten de forma positiva, interactuando respetuosamente con la escuela y entre sí en las redes sociales, del mismo modo que lo harían cara a cara.

Este comportamiento positivo puede resumirse en no hacer ninguna publicación que sea o pueda interpretarse como intimidatoria, agresiva, grosera, insultante, ilegal o inapropiada por cualquier otro motivo, o que pueda desacreditar a la escuela o (especialmente en el caso del personal) a la profesión docente. Esto se aplica tanto a las páginas públicas como a los mensajes privados, por ejemplo, chats de familias, páginas o grupos.

Si las familias tienen alguna duda sobre la escuela, les rogamos que se pongan en contacto con nosotros directamente y en privado para resolver el asunto. Si el problema no puede resolverse de este modo, debe seguirse el procedimiento de quejas de la escuela. Compartir las quejas en las redes sociales es poco probable que ayude a resolver el asunto, pero puede causar disgustos al personal, al alumnado y a las familias, además de minar la moral del personal y la reputación de la escuela, lo cual es importante para el alumnado a los que atendemos.

La escuela tiene una cuenta oficial en Twitter y puede responder a preguntas generales sobre la escuela, pero pide a las familias/cuidadores que no utilicen este canal para comunicarse sobre sus hijos. El correo electrónico es el único canal de comunicación electrónica aceptado entre las familias y la escuela, y entre el personal y el alumnado.

Se recuerda al personal que tiene la obligación de no desacreditar a la escuela ni a la profesión, y que la forma más fácil de evitarlo es tener los ajustes de privacidad más estrictos y evitar compartir información inapropiada y excesiva en línea. Nunca deben hablar de la escuela o de sus partes interesadas en las redes sociales y deben tener cuidado de que sus opiniones personales no se atribuyan a la escuela, la fundación o la autoridad local, desprestigiando a la escuela.

14. Uso del dispositivo

El uso de teléfonos móviles está regulado en la política específica (Política de uso de teléfonos móviles)

En caso de discrepancias sobre la interpretación, prevalecerá la versión original en español.

Revisado el 19/02/2024 por el equipo de salvaguardia y el equipo directivo.

Anexo 1

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES
ACCIÓN EDUCATIVA EXTERIOR
INSTITUTO ESPAÑOL VICENTE CAÑADA BLANCH
Growing together to achieve international success

USO DE LAS TIC

USO DE IMAGEN E INFORMACIÓN (incluyendo fotos y videos)

Como se indica en el artículo 92 de la LOPD-GDD, "los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información."

Autorizo a que la imagen de mis hijo/a sea utiliza CON FINES EDUCATIVOS en la página web oficial del centro y cuenta de twitter (ELEGIR OPCIÓN EN LAS CASILLAS A CONTINUACIÓN).

Podrá retirar su consentimiento en cualquier momento contactando con la Secretaría del Colegio en la siguiente dirección: canada.blanch.uk@educacion.gob.es

WEB: ☐ Doy mi consentimiento. ☐ No doy mi consentimiento.

TWITTER: ☐ Doy mi consentimiento. ☐ No doy mi consentimiento.

Londres a ..... de ..... de 20.....

☐ **DECLARO RESPONSABLEMENTE, en virtud del art. 69 Ley 39/2015, que todos los datos arriba expuestos son verídicos y que toda la documentación justificativa que adjunto es original o copia de documentación original.**

NOMBRE Y APELLIDOS DEL DECLARANTE (PADRE / MADRE O TUTOR LEGAL DEL ALUMNO)

Anexo 2

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES
ACCIÓN EDUCATIVA EXTERIOR
INSTITUTO ESPAÑOL VICENTE CAÑADA BLANCH
Growing together to achieve international success

ACUSE DE RECIBO DE LAS POLÍTICAS DE TIC

NOMBRE DEL PERSONAL: .....

- ❑ Confirmo que he leído y comprendido la política de seguridad electrónica.
- ❑ Confirmo que sé quién es el Responsable de TIC y los Coordinadores de TIC.
- ❑ Confirmo que he recibido formación en tecnologías TIC y seguridad electrónica.
- ❑ Confirmo que conozco el procedimiento en caso de que surja algún problema.

Todo el personal de la escuela es un miembro valioso de la comunidad escolar. Se espera de todos ellos que establezcan y mantengan los más altos niveles de exigencia en su propia actuación, que trabajen en equipo y que sean un excelente modelo para los niños en su propio uso de la tecnología.

Entiendo que como miembro del personal de la escuela debo:

- ❑ Comprenda que la seguridad en línea es una parte fundamental de la protección; como tal, forma parte del trabajo de todos: nunca piense que otra persona se encargará de ello.
- ❑ Identificar oportunidades para encauzar la seguridad en línea a través de todas las actividades escolares, tanto fuera del aula como dentro del plan de estudios, apoyando a los responsables del plan de estudios/etapas/asignaturas y aprovechando al máximo las oportunidades de aprendizaje inesperadas que surjan.
- ❑ Siempre que supervise el uso de la tecnología en la escuela o en tareas escolares, fomente un uso sensato, controle lo que hace el alumnado y tenga en cuenta los posibles peligros y la adecuación a la edad de los sitios web.
- ❑ Supervisar y guiar cuidadosamente al alumnado cuando participen en actividades de aprendizaje que impliquen el uso de tecnología en línea (incluidas las actividades extraescolares y de extensión escolar).
- ❑ Apoyar al alumnado en la capacidad de búsqueda, el pensamiento crítico y cuestiones jurídicas como los derechos de autor y la legislación sobre datos.
- ❑ Adopte un planteamiento de tolerancia cero frente a la intimidación y el acoso sexual de bajo nivel.

Firma.....Fecha .....

Por favor, firme y devuelva este formulario al *Designated Safeguarding Lead*:

Firma DSL .....Date.....