



CONSEJERÍA DE EDUCACIÓN  
INSTITUTO ESPAÑOL  
VICENTE CAÑADA BLANCH

# Cañada Blanch Spanish School

Founded 1972



## Política de Protección de Datos

Revisada 28/11/2019

Instituto Español Vicente Cañada Blanch  
317 Portobello Road  
London W10 5SZ  
Tel: 020 8969 2664  
[canada.blanch.uk@educacion.gob.es](mailto:canada.blanch.uk@educacion.gob.es)  
<http://vicentecanadablanch.educalab.es/>

## Introducción

En este documento explicamos qué datos personales obtenemos y tratamos, cómo los obtenemos, qué hacemos con ellos, cómo los almacenamos, a quién los transferimos, cómo gestionamos sus derechos de protección de datos y cómo cumplimos con la normativa sobre protección de datos.

## Referencias normativas

La presente política de Protección de Datos está basada en la siguiente normativa:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

## Por qué recogemos y usamos los datos de nuestro alumnado

Recopilamos y utilizamos la información del alumnado para asegurarnos de que estén protegidos y logren el mejor resultado posible del tiempo en el centro. También necesitamos esta información para cumplir nuestras obligaciones legales con las autoridades locales y las familias.

Utilizamos los datos recopilados para:

- Apoyar el aprendizaje
- Supervisar e informar sobre el progreso del alumnado
- Proporcionar un cuidado pastoral apropiado
- Evaluar la calidad de nuestros servicios
- Cumplir con la ley en lo que se refiere a la transmisión de datos

## Qué datos obtenemos

Bajo el [Reglamento General de Protección de Datos de la UE de 2018 \(GDPR\)](#), los centros educativos, en el ejercicio de sus funciones, no necesitan el consentimiento expreso de los titulares de los datos para su tratamiento en el ejercicio de la función educativa, y lo deben hacer respetando su privacidad e intimidad .

Los datos que recogemos son:

- Información personal (incluyendo nombre, número y dirección del alumno o alumna, parientes cercanos, cartas de los padres y madres, información de colegios anteriores, otras agencias tales como terapeutas del habla y del lenguaje, guarderías infantiles).
- Características (como el origen étnico, el idioma, la nacionalidad, el país de nacimiento, las necesidades de aprendizaje y el derecho a comidas escolares gratuitas).
- Información sobre asistencia (como sesiones a las que asistió, número de faltas y motivos de absentismo).
- Información sobre el comportamiento, las exclusiones y los incidentes racistas
- Información médica (como diagnósticos, medicamentos e informes relacionados de profesionales médicos)
- Los resultados de las pruebas y el progreso del alumno o alumna

## Cómo obtenemos los datos

Los datos se obtienen a través de los formularios impresos de solicitud de admisión y matrícula que rellenan las familias al inscribir a sus hijos/as en nuestro centro. Aunque la mayor parte de la información sobre los alumnos y alumnas que se nos proporciona es obligatoria, parte de ella se nos cede de forma voluntaria. Con el fin de cumplir con el Reglamento General de Protección de Datos, informaremos si es necesario que se nos proporcione cierta información sobre el alumno o alumna o si tiene la opción de hacerlo.

## Cómo tratamos los datos

SISTEMA DE GESTIÓN DE DATOS. Los datos recogidos a través de los formularios se graban en **Alborán**, el sistema estándar de gestión académica del Ministerio de Educación, Cultura y Deporte usado en Ceuta y Melilla, construido y gestionado por el INTEF. Se trata de un sistema de planificación de recursos empresariales (ERP) donde se almacenan todos los datos de los centros adscritos al proyecto del Sistema Educativo Digital <http://sed.educalab.es/proyecto>

MEDIOS DE DIFUSIÓN y REDES SOCIALES. Nuestro centro centraliza toda la difusión de imágenes y información únicamente a través de los siguientes canales oficiales:

- **Página web** <http://vicentecanadablanch.educalab.es/>. Se aloja en Sistema Educativo Digital (SED) del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF).

El INTEF es la unidad del Ministerio de Educación y Formación Profesional responsable de la integración de las TIC y la Formación del Profesorado en las etapas educativas no universitarias. Tiene rango de Subdirección General integrada en la Dirección General de Evaluación y Cooperación Territorial que, a su vez, forma parte de la Secretaría de Estado de Educación y Formación Profesional.

El SED es un conjunto de aplicaciones interconectadas que proveen de todos los servicios que requiere un centro docente para la consecución de los objetivos del currículum, la personalización de la enseñanza, la mejora de la calidad de los aprendizajes y de la comunicación con las familias. Tienen más información en el siguiente enlace <http://sed.educalab.es/proyecto/sed>

- **Cuenta oficial de Twitter @Canada\_Blanch.** Twitter es un servicio de microblogging y redes sociales en el que los usuarios publican e interactúan con mensajes conocidos como "tweets". Los tweets estaban restringidos originalmente a 140 caracteres, pero el 7 de noviembre de 2017, este límite se duplicó a 280. La política de protección de datos de Twitter cumple con el (RGPD) y puede consultarse en el siguiente enlace <https://twitter.com/es/privacy>.
- **Canal de Youtube Instituto Español Vicente Cañada Blanch** <https://www.youtube.com/channel/UCD89e0ITbpryadsS1MJ4lhg>. Forma parte de los servicios incluidos en la plataforma G suite for Education de google del centro bajo el dominio @ievcb Blanch. Más información en [https://gsuite.google.com/terms/education\\_privacy.html?hl=es](https://gsuite.google.com/terms/education_privacy.html?hl=es) y en [https://edu.google.com/intl/es-419/k-12-solutions/privacy-security/?modal\\_active=none](https://edu.google.com/intl/es-419/k-12-solutions/privacy-security/?modal_active=none)

CORREOS ELECTRÓNICOS. Para las comunicaciones con las familias, personal del centro y alumnado, se utilizan exclusivamente los correos oficiales del Ministerio y/o corporativo del centro:

- **Correo oficial @educacion.gob.es.** Lo proporciona el Ministerio de Educación y Deporte a través de Microsoft Outlook. En este espacio se pone a disposición de todas las unidades del Ministerio información y recursos útiles relativos a la Protección de Datos de Carácter Personal y el Reglamento General de Protección de Datos (RGPD): <https://extranet.mecd.es/mis-servicios-electronicos/.DanaInfo=.aiovuesk0HvonpMs7+pr oteccion-datos-caracter-personal.html>
- **Correo corporativo @ievcb Blanch.** Lo proporciona el colegio a través de la plataforma G suite for Education de google. El centro tiene configurado los permisos más restrictivos que impiden compartir archivos con miembros ajenos a la organización y el compromiso de Google de **cumplir el RGPD** en todos los servicios de G Suite para Centros Educativos. Más información en [https://gsuite.google.com/terms/education\\_privacy.html?hl=es](https://gsuite.google.com/terms/education_privacy.html?hl=es) y en [https://edu.google.com/intl/es-419/k-12-solutions/privacy-security/?modal\\_active=none](https://edu.google.com/intl/es-419/k-12-solutions/privacy-security/?modal_active=none)

## Plataformas educativas de gestión académica

En ocasiones se utilizan aplicaciones de gestión académica. Únicamente utilizamos las que ofrecen información claramente definida sobre los tratamientos efectuados, las finalidades de los mismos y sus responsables, así como sobre la ubicación de los datos, el periodo de retención, y las garantías con relación a su seguridad.

Las aplicaciones educativas, que pueden ser de gran utilidad para el aprendizaje así como para la organización de las aulas, se incluyen anualmente en nuestra política de seguridad, debiendo el profesorado solicitar, previamente a su utilización, la autorización del centro, que conlleva la evaluación de la aplicación desde el punto de vista de la seguridad de la información y la consiguiente autorización o denegación por parte del Centro. Los criterios que se aplican para autorizar su uso se recogen al final de la Política, en el Anexo Evaluación de Aplicaciones.

En todo caso, las aplicaciones que se utilicen educativamente por el alumnado deben permitir el control, por parte de los tutores o profesores, de los contenidos subidos por los menores, en especial de los contenidos multimedia (fotos, vídeos y grabaciones de voz de los alumnos).

Para la evaluación del alumnado, usamos algunas aplicaciones que implementan cuadernos de notas, agendas y organizador de clases para el profesorado. El uso de cualquiera de esas aplicaciones tendrá como único objetivo recopilar datos para la evaluación del proceso de aprendizaje del alumnado que mantienen el progreso y sus calificaciones. Estas aplicaciones, están instaladas en dispositivos protegidos por pin, contraseña, huella dactilar o cualquier otro método de bloqueo seguro y nunca se utilizarán en equipos públicos y compartidos por otros usuarios.

En ningún caso, se utilizarán estas aplicaciones para comunicarse con las familias o con el alumnado, utilizando para ello, los cauces oficiales, como el correo del instituto o el corporativo del Ministerio. Tampoco se compartirá información privada de ningún tipo a través de las mismas.

No se escribirá el nombre completo del alumnado, será suficiente con el nombre de pila y las iniciales de los apellidos, tampoco se tomarán fotos de los mismos.

Acabado el plazo de reclamaciones de notas, los datos introducidos se eliminarán.

Para más información:

<https://www.idoceo.es/index.php/es/component/content/article/10-instructions/232-politica-de-privacidad>

<https://www.additioapp.com/es/seguridad-y-privacidad/>

## Plataformas educativas de manejo de la clase/ Blogs de aula

La comunicación con las familias y el intercambio de información es un pilar fundamental de nuestro Proyecto Educativo. La creación de Blogs de aula, se convierte así en una importante herramienta para tal fin, siendo el principal objetivo, el de compartir recursos educativos con las familias

Los Blogs de aula, se crearán siempre dentro de la plataforma G suite for Education oficial del centro (Blogger y sites) y nunca desde un email personal, y en ningún caso, se difundirán fotos ni videos del alumnado en los mismos.

Por otra parte, el uso de aplicaciones para el manejo del aula (Class Dojo), se han mostrado altamente útiles para el control del grupo, dado su carácter interactivo, lúdico y de resultados inmediatos, que repercute directamente en la motivación del alumnado para trabajar responsablemente en equipo, cumplir las normas de convivencia y tener un comportamiento correcto en clase. Por tanto, el uso de este tipo de aplicaciones, tendrá una finalidad educativa y en ningún caso, se publicarán rankings ni se mostrará, a toda la clase, las puntuaciones individuales y personales. No se pondrá el nombre completo del alumnado, bastará con el nombre de pila e iniciales de los apellidos

No se establecerá ninguna comunicación con las familias, ni se compartirá ningún dato, desde este tipo de aplicaciones.

## Tratamiento de imágenes

Las fotografías tamaño carnet solicitadas con el formulario de matrícula tienen la misma consideración que los datos y, por tanto, el tratamiento que se aplica es el mismo.

El resto de fotografías y vídeos realizados al alumnado durante la actividad escolar, al no ser legalmente esenciales para la función educativa, exigen del consentimiento expreso del interesado. El artículo 4, apartado 11, del GDPR define el consentimiento como: "...cualquier indicación libre, específica, informada e inequívoca de la identidad del interesado..." que, mediante una declaración o una acción afirmativa clara, signifique para él o ella consentimiento para el tratamiento de los datos personales que le conciernen." En caso de dicho consentimiento, dicho material audiovisual será expuesto exclusivamente en los medios de difusión audiovisuales del centro ya mencionados.

En el supuesto de utilizar imágenes del alumnado para campañas de difusión y promoción del centro (vídeos promocionales, banners, etc.) se requerirá consentimiento escrito expreso de la familia.

El centro dispone de un circuito de cámaras de seguridad en los accesos al recinto escolar. Dichas grabaciones tratan de acuerdo a la normativa vigente en relación al uso de las CCTV cámaras.

## Con quién compartimos la información

No compartimos información sobre nuestros alumnos con nadie sin su consentimiento, a menos que la ley y nuestras políticas nos lo permitan. Rutinariamente compartimos información de los alumnos con:

- escuelas a las que asiste el alumno después de dejarnos
- nuestra autoridad local
- el Departamento de Educación (DfE)
- el médico de cabecera local
- Consejería de Educación en Reino Unido.
- Subdirección General de Cooperación Internacional y Promoción Exterior Educativa.

Para obtener más información sobre los requisitos de recopilación de datos que nos impone el Departamento de Educación (por ejemplo, a través del censo escolar), visite <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

Para obtener más información sobre el proceso de intercambio de datos del departamento, visite: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Para obtener información sobre las organizaciones que el departamento ha facilitado información sobre los alumnos (y para qué proyecto), visite el siguiente sitio web: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

Para más información sobre la política de protección de datos del Ministerio de Educación: <https://sede.educacion.gob.es/normativa/prot-datos-adic.html>

Para contactar con el Delegado de Protección de Datos del Ministerio de Educación: [dpd@mecd.es](mailto:dpd@mecd.es)

Para contactar a DfE: <https://www.gov.uk/contact-dfe>

## Cuánto tiempo conservamos los datos

Se espera que los miembros del personal actualicen su sistema de mantenimiento de registros utilizando el calendario de retención y que tengan en cuenta los diferentes tipos de períodos de retención cuando creen nuevos sistemas de mantenimiento de registros.

El calendario de retención se refiere a toda la información, independientemente del medio en el que esté almacenada.

Destrucción de registros. Los registros con información personal o sensible deberán ser depositados en los contenedores confidenciales habilitados a este fin y destruidos utilizando servicios profesionales de destrucción.

Transferencia de registros a los Archivos del Ministerio de Educación. Cuando se haya determinado que los registros merecen una preservación permanente, se tomarán las medidas necesarias para transferirlos a los sus dependencias.

Descripción de los archivos	Periodo de retención	Acciones a realizar al final del periodo de retención
<b>1. Dirección del centro</b>		
Informes requeridos por el Ministerio de Educación español o británico	Fecha del informe + 10 años	DESTRUCCIÓN
Correspondencia creada por los directores, equipo directivo y otros miembros del personal con responsabilidades administrativas.	Fecha de la correspondencia + 2 años	DESTRUCCIÓN
Políticas de centro	Conservar en el centro mientras siga operativa	DESTRUCCIÓN
<b>2. Alumnado / Académico</b>		
Expedientes de alumnado	Permanente	Consultar legislación para transferirlos al Ministerio de Educación
Formularios y documentación de admisión	Fecha de la solicitud + 2 años	DESTRUCCIÓN
Registros de asistencia y puntualidad	Fecha del registro + 2 años	DESTRUCCIÓN
Programaciones didácticas	Conservar en el centro mientras siga operativa	DESTRUCCIÓN
Exámenes y pruebas de evaluación	Fecha del examen + 2 años	DESTRUCCIÓN



Cartas autorización para excursiones y actividades	Año actual + 1 año	DESTRUCCIÓN
Registros de clase	Año actual + 1 año	DESTRUCCIÓN
<b>3. Health and Safety</b>		
Risk Assessments	Año actual + 3 años	DESTRUCCIÓN
Libro de registro de accidentes de primeros auxilios	Año actual + 2 años	DESTRUCCIÓN
Libros de registros documentos anti incendios	Año actual + 6 años	DESTRUCCIÓN
<b>3. Administración</b>		
Registro de entradas y salidas oficial de secretaría	Permanente	Consultar legislación para transferirlos al Ministerio de Educación
Actas de órganos de gobierno y pedagógicos (Claustro, Consejo, CCP, Departamentos, niveles, etc)	Año actual + 5 años	DESTRUCCIÓN
Registros de faltas del personal	Año actual + 1 año	DESTRUCCIÓN
Libro de registro de visitantes	Año actual + 2 año	DESTRUCCIÓN
Informes y documentos de cuerpos de inspección	Conservar mientras esté operativo y sustituir con nuevos	DESTRUCCIÓN
Circulares del Ministerio de Educación o DfES	Mientras sean necesarios para el funcionamiento	DESTRUCCIÓN
<b>4. Económico</b>		

Documentación económica exigida por la SG: Cuentas de gestión, proyectos de presupuestos, conciliación de cuentas, etc.	Año actual + 5 años	DESTRUCCIÓN
Facturas, recibos y otros documentos económicos	Año actual + 5 años	DESTRUCCIÓN
Contratos	Año de finalización + 5 años	DESTRUCCIÓN
Presupuestos de obras e informes de presupuestos	Año actual + 5 años	DESTRUCCIÓN
<b>5. Propiedad / Edificio</b>		
Documentos de propiedad	Permanente	
Planes y proyectos directores de obras	Permanente	
Informes estructurales edificio	Año actual + 6 años	DESTRUCCIÓN

## ANEXO

### EVALUACIÓN DE APLICACIONES INFORMÁTICAS

Para la evaluación de las aplicaciones desde el punto de vista de la protección de los datos personales y la seguridad de la información seguiremos las orientaciones de la Agencia Española de Protección de Datos:

**Sobre la información ofrecida por los responsables de la aplicación** se comprobará si el responsable de la aplicación informa claramente de los siguientes :

- identidad y dirección del responsable,
- las finalidades para las que serán utilizados los datos,
- las posibles comunicaciones de datos a terceros y su identidad, así como la finalidad por la que se ceden,
- los derechos que asisten a los titulares de los datos,
- la ubicación de los datos y sus periodos de conservación,
- las medidas de seguridad facilitadas por la aplicación,
- los posibles accesos que realiza la aplicación a los datos personales almacenados en el dispositivo o a sus sensores.

Esta información debería estar fácilmente accesible en la política de seguridad de la aplicación. En caso de que falte alguno de estos aspectos, o que la información facilitada no ofrezca las garantías adecuadas, no se utilizará la aplicación.

#### **Sobre la ubicación de los datos:**

Los datos deben estar almacenados en un país del Espacio Económico Europeo o un país que ofrezca un nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea). Los datos también pueden localizarse en empresas ubicadas en Estados Unidos siempre que éstas se hayan acogido a los principios del Escudo de Privacidad.

#### **Sobre la seguridad de los datos:**

La responsabilidad del cumplimiento de las medidas de seguridad debe entenderse siempre compartida entre los diferentes actores intervinientes (responsable de la aplicación, Centro Educativo y usuarios), debiendo en todo caso el responsable de la aplicación facilitar las medidas técnicas adecuadas para garantizar la seguridad de los datos tratados, y el Centro aplicarlas o utilizarlas correctamente, además de implementar las medidas organizativas apropiadas. Así, por ejemplo, la aplicación debe proveer mecanismos que permitan la realización de copias de seguridad o la descarga de los datos, de tal forma que el Centro pueda cumplir con las obligaciones que le son exigibles al respecto, introduciendo en su política de

seguridad la realización de copias de seguridad de los datos tratados mediante estas aplicaciones, y realizando efectivamente la realización de dichas copias.

La responsabilidad de las medidas de identificación de usuarios también es compartida. Por un lado, la aplicación debe implementar un mecanismo de autenticación que permita la identificación inequívoca y personalizada de los usuarios, recomendándose que este mecanismo consista en códigos de usuario y contraseñas, evitando la identificación de menores mediante datos biométricos (reconocimiento facial o huella dactilar). Si se utilizan contraseñas, el Centro requiere el cambio periódico de las mismas, por lo que las aplicaciones que se vayan a utilizar deben incluir mecanismos para permitir dichos cambios. A los usuarios les corresponde la obligación de utilizar de contraseñas robustas y custodiarlas sin desvelarlas a terceros.

### **Prueba de la aplicación:**

Se considera conveniente poner a prueba la aplicación de forma previa a su definitiva utilización en el Centro, realizando la prueba sin introducir datos personales reales de los alumnos ni involucrarlos en su utilización. En esta fase de prueba se debería comprobar la corrección de las informaciones que fueron facilitadas por el responsable de la aplicación.