



## **Política de Seguridad Digital**

Incluye la Seguridad Online, el Acuerdo sobre Seguridad Digital y el Uso de Dispositivos Propios

**Septiembre 2018**

**ELIS Villamartín**

## Contents

<b>1</b>	<b><u>INTRODUCCIÓN</u></b> .....	<b>4</b>
<b>2</b>	<b><u>OBJETIVOS DE ESTA POLÍTICA</u></b> .....	<b>4</b>
<b>3</b>	<b><u>ALUMNOS</u></b> .....	<b>5</b>
<b>4</b>	<b><u>USO NO APROPIADO POR PARTE DE LOS ALUMNOS</u></b> .....	<b>6</b>
<b>5</b>	<b><u>PERSONAL</u></b> .....	<b>6</b>
<b>6</b>	<b><u>USO NO APROPIADO POR PARTE DEL PERSONAL</u></b> .....	<b>7</b>
<b>7</b>	<b><u>PADRES Y VISITAS</u></b> .....	<b>7</b>
<b>8</b>	<b><u>ACCESO AL WI-FI</u></b> .....	<b>7</b>
<b>9</b>	<b><u>VIDEO Y FOTOGRAFÍA EN EVENTOS DEL COLEGIO</u></b> .....	<b>7</b>
<b>10</b>	<b><u>USO DE TELÉFONOS MÓVILES O DISPOSITIVOS EN INFANTIL - REGULACIONES</u></b> .....	<b>8</b>
<b>11</b>	<b><u>DISPOSITIVOS PROPIOS - BRING YOUR OWN DEVICE (BYOD)</u></b> .....	<b>8</b>
<b>12</b>	<b><u>RESPONSABILIDADES DEL COLEGIO</u></b> .....	<b>8</b>
<b>13</b>	<b><u>MEDIDAS DE FILTRADO Y PROTECCIÓN</u></b> .....	<b>8</b>
<b>14</b>	<b><u>USO DEL CORREO ELECTRÓNICO</u></b> .....	<b>8</b>
<b>15</b>	<b><u>USO DE IMÁGENES Y VIDEOS POR PARTE DEL COLEGIO</u></b> .....	<b>8</b>
<b>16</b>	<b><u>EL CURRÍCULUM Y HERRAMIENTAS DE APRENDIZAJE</u></b> .....	<b>8</b>
<b>17</b>	<b><u>SEGUIMIENTO Y CONTROL</u></b> .....	<b>9</b>
<b>18</b>	<b><u>REDES SOCIALES</u></b> .....	<b>9</b>
	<b><u>ANEXO 1: PROCEDIMIENTO EN EL CASO DE UNA INFRACCIÓN POR PARTE DE UN ALUMNO O ADULTO</u></b> .....	<b>11</b>
	<b><u>ANEXO 2: ACUERDO SOBRE SEGURIDAD DIGITAL ALUMNOS INFANTIL, YEAR 1/YEAR 2</u></b>	<b>11</b>
	<b><u>ANEXO 3: ACUERDO SOBRE SEGURIDAD DIGITAL ALUMNOS YEARS 3 A 6</u></b> .....	<b>ERROR!</b>
	<b><u>BOOKMARK NOT DEFINED.</u></b>	

**ANEXO 4: ACUERDO SOBRE SEGURIDAD DIGITAL ALUMNOS YEARS 7 – 13..... ERROR!  
BOOKMARK NOT DEFINED.**

**ANEXO 5 – POLITICA SOBRE DISPOSITIVOS PROPIOS (BYOD) ..... 16**

**ANEXO 6 - BYOD ACUERDO PADRES Y ALUMNOS..... 18**

**ANEXO 7 – PROTOCOLO CORREO ELECTRÓNICO ..... ERROR! BOOKMARK NOT DEFINED.**

### 1 Introduction

- 1.1 Esta Política de Seguridad Digital establece las funciones, responsabilidades y procedimientos para un uso aceptable, seguro y responsable de todas las tecnologías digitales y de comunicación, incluyendo el uso de los equipos del colegio, internet, correo electrónico, mensajería instantánea y demás tecnologías de redes sociales, móviles y juegos, con el fin de proteger tanto a los alumnos como a los adultos. Explica cómo el colegio ofrecerá apoyo y orientación a los padres y la comunidad en general (cuando proceda) en relación con el uso responsable de estas tecnologías. Además, también describe los procedimientos en caso de uso inaceptable o inadecuado de dichas tecnologías por parte de un adulto o un alumno.
- 1.2 El uso de Internet como una herramienta de apoyo a la enseñanza, aprendizaje y administración se ha convertido en parte integrante de la rutina en el colegio y en casa. Siempre habrá riesgos asociados al uso de cualquier tipo de comunicación que sea del dominio público. Por consiguiente, es fundamental que existan reglas, procedimientos y directrices claras que minimicen dichos riesgos cuando los alumnos hagan uso de esas tecnologías. Estos riesgos son, entre otros:
  - Vulnerabilidad ante contactos inadecuados por parte de extraños;
  - Ciberacoso;
  - Actividades ilegales de descarga o copia de material protegido por derechos de autor y uso compartido de archivos a través de Internet o los dispositivos móviles;
  - Problemas de spam y demás correos electrónicos inadecuados;
  - Contenido online abusivo, ofensivo o pornográfico;
  - Uso de las redes sociales para fomentar el extremismo; y
  - Los virus.
- 1.3 También es importante que el personal tenga claros los procedimientos, por ejemplo ponerse en contacto con los alumnos sobre los deberes solo a través de un correo electrónico del colegio o el entorno de aprendizaje virtual del colegio, como puede ser Firefly, y no mediante un correo personal.
- 1.4 Aunque nos esforzamos por protegernos y mitigar los riesgos, nunca seremos capaces de eliminarlos por completo. Cualquier incidente que se nos pudiera comunicar se tratará de inmediato de acuerdo con las políticas del colegio para garantizar que los alumnos siguen estando protegidos.
- 1.5 Es la obligación del colegio garantizar que los alumnos, profesores, personal de administración y visitantes están protegidos de cualquier posible daño mientras se encuentren en nuestras instalaciones.
- 1.6 La implicación de los alumnos y los padres también es vital para conseguir un uso correcto de las tecnologías digitales. Esta política pretende, por tanto, informar de cómo forman parte los padres y alumnos de los procedimientos, y de cómo se enseña a los alumnos a ser usuarios seguros y responsables para poder actuar con buen criterio en cuanto a la información que ven, encuentran y usan.

### 2 Objetivos de esta Política

- Garantizar la protección de todos los alumnos dentro del colegio al describir el uso adecuado y aceptable de todas las tecnologías digitales y online.
- Describir las funciones y responsabilidades de todos los alumnos, empleados y padres.
- Garantizar que todos los alumnos, empleados y padres comprenden los procedimientos en caso de uso indebido de las tecnologías online.

- Desarrollar vías de contacto con los padres y la comunidad para seguir concienciando sobre el uso de las tecnologías online.

### 3 Alumnos

#### 3.1 Nuestros alumnos:

- Están implicados en la revisión de nuestro acuerdo sobre seguridad digital a través de debates en las clases y otros foros, dependiendo de su edad;
- Son responsables de cumplir con el acuerdo sobre seguridad digital cuando estén en el colegio tal y como se acuerda cada curso académico o cada vez que un nuevo alumno comienza en nuestro colegio, y deben firmar que han leído y comprenden las normas;
- Han aprendido a utilizar Internet de manera segura y responsable, por ejemplo en las clases de informática y de PSHEE (educación personal, social, sobre salud y económica);
- Han aprendido a informar de inmediato a un adulto sobre cualquier material o contacto no adecuado de alguien a quien no conocen;
- Son conscientes del uso potencial de las tecnologías digitales online para exponer a los jóvenes a contactos inadecuados de extraños y a ideas extremistas, y saben cómo actuar de encontrarse con tales problemas;
- Han aprendido y se les anima a considerar las implicaciones de un uso indebido de internet y, por ejemplo, de subir material no adecuado a páginas web;
- Han aprendido que la descarga de materiales, como archivos de música y fotografías, debe ser correcta y adecuada a su fin, en virtud del trabajo de investigación para el colegio, y estar además libre de derechos de autor;
- Han aprendido a comprender lo que significa la seguridad online a través de una enseñanza adecuada a la edad;
- Han aprendido que enviar mensajes malintencionados o dañinos fuera del colegio puede convertirse en una cuestión sancionable por el colegio o por otros organismos tales como la policía;
- Han aprendido a no ponerse en riesgo en la red o en los teléfonos móviles y a cómo proceder si creen que se han puesto en peligro;
- Han recibido directrices y procedimientos explícitos sobre uso de móviles y otros dispositivos personales en el colegio, y se espera que cumplan la presente Política de seguridad digital; y
- Deben conectarse a internet, mientras estén en las instalaciones que posea o alquile Cognita, por medio de la red inalámbrica de los alumnos, y no deben burlar el acceso a internet usando los servicios de datos de un móvil personal.

### 4 Uso inapropiado por parte de alumnos

4.1 Si se descubriera que un alumno ha usado de manera indebida y deliberada la infraestructura digital u online del colegio, se aplicarán las sanciones correspondientes. Si un alumno accediera, de manera accidental, a contenido no adecuado, se espera de él que lo comunique al empleado de inmediato y que minimice la pantalla o cierre la ventana. Un abuso o daño intencionado a los equipos del colegio será motivo de facturación a los padres de los gastos de sustitución de dicho equipo. Si un alumno usara internet mientras no está en el colegio pero de forma que pudiera dañar a un miembro de la comunidad estudiantil, el colegio actuará de inmediato y de acuerdo con nuestras políticas de conducta.

4.2 Véase Anexo 1 para más información.

### 5 Personal

5.1 Todos los adultos del colegio son responsables de:

- Cumplir con el código de conducta del personal, incluido lo referente al uso aceptable;
- Poner en práctica el acuerdo de seguridad digital de los alumnos (véanse Anexos 2, 3 y 4);
- Tener un conocimiento actualizado sobre aspectos digitales para distintos grupos de edades;
- Permanecer alerta cuando se use la tecnología durante una clase;
- Servir de ejemplo de uso seguro y responsable de las tecnologías;
- Proporcionar recordatorios y directrices a los alumnos sobre seguridad digital;
- Garantizar que los alumnos cuentan con protección y respaldo cuando usen tecnologías online, y que saben cómo utilizarlas de forma segura y responsable;
- No dejar un ordenador u otro equipo desatendido mientras estén conectados;
- Bloquear o asegurar los equipos portátiles cuando no se estén utilizando;
- No establecer conexión con un menor de diecinueve años en ninguna red social, o a través del móvil, y seguir siempre las directrices del colegio. Véase la Política de Redes Sociales para más información.
- Preservar la confidencialidad y no revelar información de la red ni divulgar contraseñas;
  - Asegurarse de que la información sujeta a protección de datos, es decir el RGPD 2016 (y sus modificaciones o extensiones) no se almacena en medios portátiles no cifrados ni se transporta de forma no segura;
  - Mostrarse prudentes a la hora de comunicarse por vía electrónica sobre asuntos relacionados con el trabajo y no desprestigiar al colegio;
  - Cumplir con la lista de prohibiciones y permisos de la Guía de prácticas recomendables para correos electrónicos – véase Anexo 7;
  - No realizar ni responder a llamadas personales ni establecer conversaciones privadas por mensajería mientras estén trabajando;

- Comunicar cualquier preocupación sobre un alumno en relación con su protección y seguridad online al líder de protección designado;
- Comunicar cualquier acceso accidental a materiales no adecuados al informático y al DSL para que los sitios inadecuados se incluyan en la lista restringida; y
- Utilizar los equipos y tarjetas de memoria del colegio para hacer fotografías y vídeos.

### **6 Uso inapropiado por el personal**

- 6.1 Si se cree que un empleado ha hecho un uso abusivo o ilegal de internet o la red del colegio, se deberá enviar un informe al director y al DSL de inmediato. Se deben seguir los procedimientos de protección para atajar cualquier falta grave de uso, y se deberá informar a las autoridades adecuadas de ser necesario.
- 6.2 Véase Anexo 1 para más información.

### **7 Padres y Visitas**

- 7.1 Todos los padres tendrán acceso a una copia de la presente Política de Seguridad Digital a través de nuestra web. Se solicita a los padres que expliquen y hablen sobre las normas con su hijo, cuando sea posible, de manera que las entiendan y acepten sin reservas.
- 7.2 Dentro del plan para concienciar a los alumnos sobre seguridad online, el colegio podrá ofrecer a los padres la oportunidad de apoyar al colegio de manera que puedan mantener a sus hijos protegidos mientras usen las tecnologías online fuera del mismo; para ello podrán impartirse cursos para padres u ofrecerse consejos y enlaces a páginas web de utilidad. El colegio desea promover una actitud positiva en cuanto al uso de internet y, por tanto, solicita a los padres que ayuden a que sus hijos aprendan y comprendan cómo usar las tecnologías online de manera segura y responsable.
- 7.3 Los padres deberían ser conscientes de que el colegio no puede asumir la responsabilidad sobre un uso indebido o abuso por parte de un alumno de los equipos informáticos cuando no esté en el colegio. En este ámbito se incluyen las relaciones por redes sociales con otros alumnos y la posibilidad de que accedan a contenido inadecuado. No obstante, si los padres o tutores descubrieran cualquier problema, pedimos encarecidamente que se pongan en contacto de inmediato con el colegio para que podamos ofrecer nuestro apoyo y consejos. El colegio tiene la obligación de comunicar los problemas graves a los organismos locales de protección o a la policía, según dicte la ley.

### **8 Wi-Fi Access**

- 8.1 Los padres y visitantes del colegio deberán cumplir con esta política. Si los visitantes desean acceder a internet a través del Wi-Fi del colegio, se les entregará una contraseña. Tan solo se les permitirá el acceso una vez hayan accedido a cumplir con las condiciones del colegio.

### **9 Video y Fotografía en los Eventos del Colegio**

- 9.1 El colegio informará a los padres al inicio de cada evento sobre si habrá disponible un vídeo del mismo. Se solicita a los padres que tengan consideración al grabar vídeos o tomar fotografías en los eventos del colegio, y que no publiquen material de otros niños en ningún portal público sin el permiso de la familia en cuestión. Es ilegal vender o distribuir grabaciones de eventos sin permiso.

### **10 Uso de Teléfonos Móviles o Dispositivos en Infntil - Normativa**

- 10.1 Las Normas de protección y bienestar infantil (apartado 3.4) exigen a todos los colegios la instauración de una política clara sobre el uso de teléfonos y equipos móviles
- 10.2 El Código de conducta del personal de Cognita establece que “Cognita no permite el uso de teléfonos móviles ni cámaras por parte del personal cuando haya niños presentes”.

### **11 Dispositivos Propios (BYOD)**

- 11.1 Existe un procedimiento claro que regula el uso de dispositivos propios, para lo cual se debe suscribir un acuerdo con padres y alumnos. Véase anexos 5 y 6 para más información.

### **12 Responsabilidades del Colegio**

- 12.1 El colegio asume con toda seriedad sus responsabilidades en relación con el uso aceptable de la tecnología por parte de los alumnos y adultos, y entiende la importancia del control, evaluación y revisión de sus procedimientos con regularidad.

### **13 Medidas de Filtrado y Protección**

- 13.1 El sistema de internet del colegio dispone de un potente sistema de filtrado adecuado a la edad de los usuarios para filtrar el contenido no adecuado. El sistema registra todos los intentos de acceso a internet, incluso cuando se pretende acceder a contenido inadecuado.
- 13.2 La red, ordenadores de sobremesa, portátiles y tablets del colegio utilizan además filtros antivirus, antispyware, de correo basura y de spam con periodicidad. Se han implantado medidas de seguridad para garantizar que no se puede acceder a la información sobre nuestros alumnos por parte de usuarios no autorizados. Además, la red inalámbrica dispone de un cifrado reforzado que proporciona mayor seguridad.

### **14 Uso del Correo Electrónico**

- 14.1 El colegio proporciona direcciones de correo electrónico para los alumnos (Year 4-Year 13) con el fin de promover la comunicación segura y eficiente dentro del colegio. El IT Network Manager será quien proporcione las cuentas de correo.
- 14.2 Se espera que todo el personal use el correo electrónico de forma profesional y responsable. Véase Anexo 7 para más información.

### **15 Uso de Imágenes y Vídeos por parte del colegio.**

- 15.1 El colegio cumple con la legislación de protección de datos, es decir el RGPD 2016 (y sus modificaciones o extensiones) y entiende que una imagen o video se considera un dato personal. Por tanto, solicita el consentimiento por escrito a los padres para publicar imágenes y vídeos para fines de publicidad externa, como puede ser en la página web, y para fines internos, como el anuario o en el portal de los padres. Los padres y tutores pueden retirar su permiso en cualquier momento informando al equipo de administración por escrito.
- 15.2 El personal no puede utilizar sus propios equipos o tarjetas de memoria para grabar vídeos o tomar fotografías de los alumnos, y cuando se almacenen imágenes dentro de la red del colegio solo deben usar el nombre de pila del alumno.

### **16 El Curriculum y Herramientas de Aprendizaje**

- 16.1 El colegio enseña a los alumnos cómo usar internet de forma segura y responsable para recabar información, explorar conceptos, profundizar los conocimientos y comprensión o comunicarse de forma efectiva para maximizar el aprendizaje, a través de sus clases de TIC y/o PSHEE. Los siguientes conceptos, habilidades y competencias se enseñan en el colegio en consonancia con la edad de los niños:
  - Ciudadanía digital;



- Futuras habilidades laborales;
- Competencia en internet;
- Emitir opiniones sustentadas sobre páginas web y correos recibidos;
- Conocimiento de riesgos tales como los virus o leer correos de extraños;
- Acceso a recursos que describen cómo usar las tecnologías online con seguridad y responsabilidad;
- Conocimientos sobre derechos de autor y problemas de plagio;
- Compartir archivos y descargar contenido ilegal;
- Subir información, sabiendo cuál se puede subir de forma segura y que no se debe subir información personal; y
- Dónde acudir por consejo y cómo comunicar abusos.

16.2 Estas habilidades se enseñan de forma explícita dentro del programa de estudios de informática, pero también pueden cubrirse en otras asignaturas; los alumnos aprenden las habilidades necesarias para explorar cómo utilizar las tecnologías online de manera efectiva, segura y responsable. Puede encontrar más información sobre el programa de informática en la documentación del programa de estudios de informática y PSHEE.

## 17 Seguimiento y Control

- 17.1 Es responsabilidad del colegio garantizar que existen los sistemas y tecnologías adecuados para controlar y preservar la seguridad de todos aquellos que usan la red del colegio. El colegio controlará el uso de las tecnologías online e internet por parte de los alumnos y el personal. El líder de protección designado, los profesores de informática y el DSL realizarán auditorías habituales con los alumnos para evaluar sus conocimientos y comprensión de cuestiones relacionadas con la seguridad online, y actuarán en aquellas áreas de mayor vulnerabilidad.
- 17.2 A la hora de auditar la seguridad digital y la efectividad de esta política se debe tener en cuenta lo siguiente:
- ¿Ha sido efectivo el registro de incidentes sobre seguridad online? ¿Se mantienen registros?
  - ¿Fue capaz el colegio de responder de manera efectiva a los incidentes?
  - ¿Se resolvieron los incidentes de la mejor forma que le posible al colegio?
  - ¿Todos los alumnos demuestran estar concienciados sobre la seguridad online de acuerdo con su edad?
  - ¿Se han registrado y resuelto las quejas o preocupaciones sobre la política?
  - ¿Se han dado avances tecnológicos que deberían tratarse bien en el programa o dentro de la formación para la concienciación?
  - ¿Todos los empleados entienden la política y la consideran adecuada y viable?

- ¿Es adecuada la formulación actual y refleja el uso de las tecnologías en el colegio?
- ¿Saben todos los miembros de la comunidad escolar cómo informar de un problema?
- ¿Se respeta la seguridad online durante las clases y está presente en los documentos del programa didáctico?

### **18 Redes Sociales**

18.1 Para consejos relacionados con el uso de las redes sociales véase la Política de Redes Sociales.

### Anexo 1: Procedimientos para personal en caso de una infracción de esta política por parte de un adulto o alumno.

- (A) Se ha accedido de manera involuntaria a una página web inadecuada:
- Informar al informático y al DSL; y
  - Contactar al Técnico Informático por correo electrónico para que se añada a la lista de páginas prohibidas o restringidas.
- (B) Se ha accedido de manera voluntaria a una página web inadecuada:
- Asegurarse de que nadie más puede acceder al material apagando el ordenador;
  - Registrar el incidente por escrito;
  - Informar al director y al DSL de inmediato; y
  - El director aplica la política de conducta.
- (C) Un adulto recibe material no adecuado:
- No reenviar dicho material a nadie más, de lo contrario podría constituir un delito;
  - Avisar al director y al DSL de inmediato; y
  - Asegurarse de que el equipo se apaga y registrar la naturaleza del material.
- (D) Un adulto ha utilizado los equipos informáticos de manera inadecuada:
- Seguir los mismos procedimientos que en (B).
- (E) Un adulto se ha puesto en contacto con un alumno o usado los equipos informáticos de manera inadecuada:
- Asegurarse de que el alumno se ha tranquilizado;
  - Informar al director, que debería seguir el código de conducta de los empleados y la política de protección (si corresponde);
  - Guardar la información que ha recibido el alumno, de ser posible, y decidir si es ofensiva, intimidatoria o inofensiva; y
  - Si se decide que ha existido un uso ilegal o inadecuado, informar al director (o a la *Education Adviser Spain*, si la acusación va dirigida contra el director) y al DSL de inmediato, y seguir la política de *Safeguarding*.
- (F) Se suben a la página web del colegio comentarios amenazantes o maliciosos, o bien se distribuyen a través del correo del colegio (o se imprimen), en relación con un adulto del colegio:
- Conservar las pruebas; y
  - Informar al director de inmediato y seguir la política de protección, según sea necesario.
- (G) Cuando se publican imágenes de empleados o adultos en páginas web inadecuadas, o se sube información inadecuada sobre ellos en cualquier sitio:
- Se debe informar al director.

### Anexo 2 – Acuerdo sobre Seguridad Digital para alumnos de Infantil, Year 1 & Year 2

#### Infantil, Year 1 & Year 2: Acuerdo sobre seguridad digital

Estas son las normas para un uso seguro y responsable de internet en el colegio:

- Utilizamos internet de forma segura para ayudarnos a aprender.
- Aprendemos cómo usar internet.
- Si vemos algo en internet o recibimos un mensaje que es desagradable, debemos informar a un adulto.
- Aprendemos a mantener secreta nuestra contraseña.
- Sabemos a quién y cuándo pedir ayuda.
- Si vemos algo en el ordenador que no nos gusta o que nos hace sentir incómodos, sabemos qué hacer.
- Sabemos que es importante cumplir las normas.
- Cuidamos los unos de los otros mediante un uso seguro de internet.

### Anexo 3 – Acuerdo sobre Seguridad Digital para alumnos Year 3 - 6

#### Years 3 - 6: Acuerdo sobre seguridad digital

Estas son las normas para un uso seguro y responsable de internet en el colegio:

- Usamos internet para ayudarnos a aprender, y aprendemos cómo usar internet de forma segura y responsable.
- Enviamos correos y mensajes amables.
- Puede que necesitemos autorización de un adulto para enviar un correo, chatear o hablar por videoconferencia con alguien del colegio.
- Nunca mostramos contraseñas ni información personal (como nuestro apellido, dirección o número de teléfono).
- Nunca subimos fotografías ni vídeos sin el permiso del profesor, y nunca incluimos nombres con las fotografías.
- Si necesitamos ayuda, sabemos a quién y cuándo pedirla.
- Si vemos algo en internet o recibimos un mensaje o correo electrónico que es desagradable o nos hace sentirnos incómodos, informamos a un adulto.
- Acepto que los monitores del colegio pueden controlar mi uso de internet en el colegio y mi cuenta de correo electrónico del colegio.
- Si recibimos un mensaje de un desconocido, informamos a un adulto.
- Cuidamos los unos de los otros mediante un uso seguro y responsable de internet.
- Aceptamos no enviar palabras, imágenes o mensajes hirientes fuera del colegio, por internet o por móvil, sobre nadie de nuestra comunidad escolar.

Nombre: \_\_\_\_\_ Curso: \_\_\_\_\_

Entiendo el acuerdo sobre seguridad digital para un uso seguro y responsable de internet, el correo electrónico y las herramientas online. Soy consciente de que los adultos que trabajan conmigo en el colegio me ayudarán a comprobar si uso el ordenador de forma adecuada.

Firma del alumno: \_\_\_\_\_ Fecha: \_\_\_\_\_

### Anexo 4 – Acuerdo sobre Seguridad Digital para alumnos de Years 7 - 13

#### Years 7 - 13: Acuerdo sobre seguridad digital

Se me anima a usar y conocer las normas y procedimientos de seguridad que regulan mi uso de los recursos TIC, incluyendo internet. El acceso a la red e internet del colegio me permite encontrar recursos, comunicarme y me facilita la investigación a la hora de realizar las tareas escolares.

Acepto que estos servicios deben utilizarse solo para fines educativos y de manera adecuada. Asumo la responsabilidad de mis acciones y sé que el incumplimiento de las normas se considerará una falta de disciplina grave.

- Utilizaré internet de forma selectiva como apoyo a mis estudios.
- Acepto que los monitores del colegio pueden controlar mi uso de internet en el colegio y mi cuenta de correo electrónico del colegio.
- Si traigo equipos personales al colegio, incluyendo móviles, acepto acceder a internet a través de la red Wi-Fi del colegio.
- No accederé, crearé ni divulgaré material (imágenes, sonidos, texto, vídeos) que pueda ser motivo de ofensa, incomodidad o ansiedad para otra persona.
- Seguiré todas las instrucciones de mis profesores en cuanto al uso de las TI e internet.
- No doy por sentado que la información publicada en una web o escrita en un correo electrónico sea verdadera.
- Preservo la confidencialidad de mi nombre de usuario y contraseña.
- Llevo cuidado con lo que escribo en el ordenador. Compruebo mi trabajo antes de imprimirlo o enviarlo.
- No utilizo lenguaje inapropiado. No escribo palabras racistas, sexistas, insultantes, homofóbicas o agresivas. No escribo cosas que pudieran molestar u ofender a otros.
- Entiendo que enviar mensajes maliciosos fuera del colegio puede ser objeto de sanción por parte del colegio o implicar a otros organismos externos, como la policía.
- Soy consciente de que mi actividad online nunca debe molestar ni herir a otras personas, y que no debería ponerme en riesgo a mí mismo.
- No divulgo información personal, ni mía ni de otras personas (como pudieran ser direcciones, números de teléfono o datos privados), a través de correos electrónicos o en páginas web.
- No respondo a mensajes ofensivos, insultantes o groseros. Informo a un profesor de inmediato si recibo algo con lo que no me siento cómodo.
- En el colegio no visito páginas ni descargo materiales que son de mal gusto, ofensivos, violentos o pornográficos.
- Si cito un texto, siempre mencionaré mis fuentes y reconozco el uso de las ideas, imágenes o datos de otros citando al autor, usando comillas e incluyendo la bibliografía, según se requiera.

## Política de Seguridad Digital

---

- Siempre respeto la privacidad de los datos de otros usuarios.
- Comunicaré a un profesor cualquier incidente que incumpla el acuerdo sobre seguridad digital, incluso aunque el incidente no me afecte a mí.
- Trataré con cuidado los equipos de TI del colegio y comunicaré cualquier daño a un profesor.
- Si daño de forma deliberada un equipo del colegio, se me cobrará su sustitución.
- No desprestigiaré el nombre del colegio al usar los equipos de TI o el correo electrónico del mismo.
- Comprobaré mis correos del colegio con regularidad para poder trabajar y aprender de forma efectiva.
- Seguiré las normas del colegio sobre honradez académica y no copiaré.
- Sé que si tengo alguna duda tecnológica fuera del colegio puedo pedir ayuda o consejo a mis profesores.

Nombre: \_\_\_\_\_ Curso: \_\_\_\_\_

Entiendo el contenido del acuerdo sobre seguridad digital y las normas para un uso seguro y responsable de internet, el correo electrónico y las herramientas online. Soy consciente de que los adultos que trabajan conmigo en el colegio me ayudarán a comprobar si uso el ordenador de forma adecuada.

Firma del alumno: \_\_\_\_\_ Fecha: \_\_\_\_\_

### Anexo 5 – Política sobre Dispositivos Propios (BYOD)

#### Introducción

Nuestro objetivo es estar a la vanguardia en el desarrollo de una política digital significativa, flexible y participativa que mejore nuestra ya excelente oferta educativa. Tenemos claro que el mejor recurso es tener en cada clase un profesor altamente cualificado, bien informado y entusiasta. A través de nuestra estrategia digital, pretendemos ampliar las destrezas y experiencia educativa del colegio de manera que nuestros alumnos y empleados estén preparados para un mundo digital en constante cambio. Creemos firmemente que al ofrecer recursos y oportunidades adicionales por medio del entorno digital nuestros alumnos progresarán a nivel académico y estarán más preparados a la hora de estudiar cualquier carrera. El uso de dispositivos puede intensificar el aprendizaje. No obstante, los alumnos que opten por no usar equipos tampoco tienen por qué retrasarse en sus estudios.

#### Vínculos con otras políticas

Esta política debe leerse en conjunción con otras políticas tales como el Código de conducta del personal, el Acuerdo sobre Seguridad Digital y la Política de *Safeguarding*.

#### Objetivo

Nuestro objetivo consiste en permitir a los alumnos utilizar su propio dispositivo de forma segura para maximizar su aprendizaje. Para ello es posible que se deba usar un ordenador propio en apoyo a su estudio independiente o, si así lo sugiere el profesor, para las clases escolares.

#### Cursos a los que se aplica

Esta política está destinada a alumnos mayores de 16 años de KS 4 y 5. Es posible que se permita usar su propio equipo a alumnos del segundo ciclo de primaria y de secundaria (para clases concretas), en cuyo caso también debe seguirse esta política.

Será el profesor quien decida si se debe usar cualquier dispositivo, y los alumnos deberán actuar tal y como se les conmina. Si los alumnos incumplieran o hicieran un uso indebido de la presente política, se deberá aplicar la política de conducta del colegio.

#### Información para alumnos y padres/tutores

- Antes de llevar el dispositivo al colegio por primera vez, los alumnos y sus padres o tutores deben leer esta política, que establece las responsabilidades y expectativas relativas al uso de los dispositivos personales. Al traer el dispositivo al colegio, tanto los alumnos como los padres y/o tutores están aceptando las condiciones de la presente política.
- Los alumnos deben utilizar su equipo en cumplimiento del acuerdo de seguridad digital del colegio.
- Los alumnos seguirán las directrices del profesor en cuanto al uso adecuado de sus dispositivos en clase y no deben usarlos a menos que así se lo indique. El uso de un dispositivo sin permiso implicará su confiscación y el padre y/o tutor deberá recogerlo de recepción según dictamina la política del colegio sobre dispositivos móviles.
- Los alumnos deben conectar su dispositivo a la red de datos inalámbrica del colegio, y no deben esquivarla y sustituirla por otra red distinta a la del colegio.
- El uso del dispositivo durante horario escolar será decisión del profesor y del personal. Los alumnos deberán usar sus dispositivos tan solo si así lo indica el profesor.
- El dispositivo solo debe usarse para fines educativos.



- Los dispositivos deben estar silenciados en todo momento.
- Los dispositivos deben permanecer en los bolsillos o mochilas a menos que el profesor permita su uso.
- Los dispositivos deben traerse al colegio totalmente cargados. El colegio no ofrece medios de carga.
- Cada alumno será responsable exclusivo del cuidado de su dispositivo y de su conducta mientras lo use en todo momento, ya sea en el colegio como en casa o en cualquier parte.
- Los alumnos deben poder identificar con claridad su dispositivo.
- Los dispositivos podrán usarse durante los recreos/almuerzo. Pueden usarse fuera de los edificios.
- Todos los dispositivos deberían guardarse bajo llave en las taquillas durante las clases de educación física o durante los juegos.
- Los dispositivos deberían estar cubiertos por una póliza de seguro en vigor.
- Si se incumple la presente política, incluso si suena o se usa un móvil durante una clase, el dispositivo se confiscará y se guardará en la Secretaría hasta finalizar la jornada escolar. Si se incumplen las normas de manera reiterada, es posible que se prohíba al alumno traer el dispositivo al colegio.
- El acuerdo sobre seguridad digital del colegio se aplica a todos los alumnos que usen cualquier dispositivo en el colegio. Todos los alumnos deben cumplir esta política sin falta.
- El dispositivo debe contar con un software antivirus adecuado, válido y activo.
- Nunca se debe esperar que los alumnos cuenten con un dispositivo. El uso del dispositivo debe ser accesorio a una enseñanza excelente.
- El colegio no asume responsabilidad alguna en relación con las pérdidas o daños que sufran los dispositivos mientras estén en el colegio o cuando se realicen actividades en el exterior.
- La decisión sobre traer dispositivos al colegio recae en los alumnos y sus padres/tutores, al igual que la responsabilidad en caso de pérdida o daño derivado del uso del dispositivo en el colegio.
- Los profesores deben fomentar y facilitar el uso de los dispositivos personales en las clases solo cuando lo crean conveniente. El uso de los dispositivos por parte de los alumnos queda a total discreción del profesor.
- Los profesores deben seguir procedimientos disciplinarios estándar si un alumno usa un dispositivo sin permiso.
- Todos los alumnos que han sido designados por el departamento de orientación podrán usar sus dispositivos cuando sea apropiado.
- El SENCO informará al personal si se les permite a los alumnos usar los dispositivos en las clases por motivos médicos y/o de accesibilidad, para permitirles acceder al programa escolar.

### Información sobre las funciones del colegio

El colegio:

- Espera que todos los alumnos que traigan su propio dispositivo se conecten a la red inalámbrica filtrada del colegio;
- No ayudará a los alumnos a establecer la conexión de red con su propio dispositivo;
- No asume responsabilidad alguna ante cualquier pérdida o daño, o mantenimiento o reparación de los dispositivos de los alumnos; y
- No ofrece cobertura de seguro para los dispositivos que se traigan a clase.

### Dispositivos adecuados

- Los dispositivos deberán llevarse encima durante toda la jornada escolar, con lo que es importante que sean ligeros. El colegio soporta sistemas Apple y Windows.
- Los dispositivos deben ser compatibles con cualquiera de los siguientes navegadores: Windows Edge, Internet Explorer, Firefox, Chrome y Safari.
- Los dispositivos deben estar cargados antes de traerlos al colegio.

## Anexo 6 – Acuerdo de padres/alumno sobre dispositivos propios BYOD

### Padres/tutores legales

El colegio no asume la responsabilidad en caso de pérdida o daños de dispositivos personales cuando se encuentren en el colegio, fuera del colegio o durante actividades en el exterior. La decisión de traer un dispositivo al colegio recae en el alumno y sus padres y/o tutores, al igual que la responsabilidad en caso de pérdida o daño derivado del uso del dispositivo en el colegio. Una condición indispensable para que los alumnos puedan traer su dispositivo al colegio es que el padre y/o tutor suscriba esta política sobre dispositivos propios aceptando así esta exoneración de responsabilidad.

### Dispositivo propio – Información para padres y/o tutores

- Nunca se debe esperar que los alumnos cuenten con un dispositivo. El uso del dispositivo debe ser accesorio a una enseñanza excelente.
- El colegio no asume responsabilidad alguna en relación con las pérdidas o daños que sufran los dispositivos mientras estén en el colegio, fuera del colegio o cuando se realicen actividades en el exterior.
- La decisión sobre traer dispositivos al colegio recae en los alumnos y sus padres/tutores, al igual que la responsabilidad en caso de pérdida o daño derivado del uso del dispositivo en el colegio.
- Los dispositivos deberían estar cubiertos por una póliza de seguro en vigor.
- El acuerdo sobre seguridad digital del colegio se aplica a todos los alumnos que usen cualquier dispositivo en el colegio. Todos los alumnos deben cumplir esta política sin falta.
- Cada dispositivo debe contar con un software antivirus adecuado, válido y activo.

He leído la política sobre dispositivos propios y doy mi autorización para el uso de dispositivos propios en el colegio. Entiendo que el colegio no asume responsabilidad alguna en relación con los dispositivos que usen los alumnos en el colegio. He leído el acuerdo sobre seguridad digital y apoyaré al colegio en su cumplimiento.

Nombre (Padre/madre/tutor)

.....

Firma

.....

.....

Fecha

.....

.....

### Dispositivo propio – Información para alumnos

- Antes de llevar el dispositivo a clase por primera vez, los alumnos y sus padres/tutores deberán leer este acuerdo, el cual establece las responsabilidades y expectativas derivadas del uso de los dispositivos. Al llevar el dispositivo al colegio, los alumnos y los padres/tutores estarán aceptando las condiciones de la presente política y del acuerdo sobre seguridad digital.
- Los alumnos deben seguir las directrices de los profesores en cuanto al uso adecuado de sus dispositivos en clase, y solo deberán utilizarlos cuando así se lo indique el profesor. El uso de

los dispositivos sin permiso implicará su confiscación, y el padre o tutor deberá recogerlo en la oficina del colegio según dictamine la política del colegio sobre dispositivos móviles.

- Los alumnos deben conectar su dispositivo a la red inalámbrica del colegio y no deben usar una RPV.
- El uso del dispositivo propio durante la jornada escolar es decisión única y exclusiva del profesor y el personal. Los alumnos solo deberán utilizar el dispositivo cuando así se lo indique el profesor.
- El dispositivo debería usarse solo con fines educativos.
- Los teléfonos deben permanecer silenciados en todo momento.
- Los teléfonos deben permanecer en los bolsillos o mochilas a menos que el profesor permita su uso.
- Los dispositivos deben traerse al colegio totalmente cargados. El colegio no ofrece medios de carga.
- Cada estudiante será único responsable de su propia conducta y del cuidado de su dispositivo en todo momento, ya sea mientras está en el colegio, en casa o en cualquier otra parte.
- Los alumnos deben poder identificar con claridad su dispositivo.
- Los dispositivos deben usarse durante los recreos/almuerzo. Pueden usarse fuera de los edificios.
- Todos los dispositivos deberían guardarse bajo llave en las taquillas durante las clases de educación física o durante los juegos.
- Si se incumple la presente política, incluso si suena o se usa un móvil durante una clase, el dispositivo se confiscará y se entregará a la oficina del colegio hasta que finalice la jornada escolar. Si se incumplen las normas de manera reiterada, es posible que se prohíba al alumno traer el dispositivo al colegio.
- El dispositivo debe contar con un software antivirus adecuado, válido y activo.
- En última instancia, la decisión sobre si se ha utilizado un dispositivo de forma indebida recae única y exclusivamente sobre el profesor o un miembro de la plantilla del colegio.

### Seguridad digital para alumnos

Se me anima a cumplir y conocer las normas y procedimientos de seguridad que regulan el uso de los dispositivos, incluido internet. El acceso a la red del colegio e internet me permite encontrar recursos, comunicarme de forma adecuada (de acuerdo con esta política) y me ayuda en la investigación para realizar mis tareas escolares. Acepto que estos servicios deben usarse solo con fines educativos y de manera adecuada. Asumo la responsabilidad de mis acciones y sé que cualquier incumplimiento de las normas se considerará una falta de disciplina grave.

- Acepto que el colegio controle el uso que hago de internet en el colegio así como mi cuenta de correo electrónico del colegio.

- Si traigo un dispositivo al colegio, incluyendo un móvil, me comprometo a acceder a internet a través del Wi-Fi del colegio pero solo si así lo indica el profesor.
- No accederé, crearé ni divulgaré material (imágenes, sonidos, texto, vídeos) que pueda ser motivo de ofensa, incomodidad o ansiedad para otra persona.
- Seguiré todas las instrucciones de mis profesores en cuanto al uso de mi dispositivo e internet.
- No doy por sentado que la información publicada en una web o escrita en un correo electrónico sea verdadera.
- Preservaré la confidencialidad de mi nombre de usuario y contraseña.
- Llevaré cuidado con lo que escribo en el ordenador. Comprobaré mi trabajo antes de imprimirlo o enviarlo.
- No utilizaré lenguaje inapropiado ni escribiré palabras racistas, sexistas, insultantes, homofóbicas o agresivas. No escribiré cosas que pudieran molestar u ofender a otros.
- Entiendo que enviar mensajes maliciosos fuera del colegio puede ser objeto de sanción por parte del colegio o implicar a otros organismos externos, como la policía.
- Soy consciente de que mi actividad online nunca debe molestar ni herir a otras personas, y que no debería ponerme en riesgo a mí mismo.
- No divulgaré información personal, ni mía ni de otras personas (como pudieran ser direcciones, números de teléfono o datos privados), por ningún medio.
- No responderé a mensajes ofensivos, insultantes o groseros. Informaré a un profesor de inmediato si recibo algo con lo que no me siento cómodo.
- En el colegio no visitaré páginas ni descargaré materiales que sean de mal gusto, ofensivos, violentos o pornográficos.
- Si cito un texto, siempre mencionaré mis fuentes y reconoceré el uso de las ideas, imágenes o datos de otros citando al autor, usando comillas e incluyendo la bibliografía, según se requiera.
- Siempre respeto la privacidad de los datos de otros usuarios.
- Comunicaré a un profesor cualquier incidente que incumpla las normas sobre seguridad digital, incluso aunque el incidente no me afecte a mí.
- Trataré con cuidado los dispositivos de otros alumnos y equipos TIC del colegio y comunicaré cualquier daño a un profesor.
- Si daño de forma deliberada un equipo del colegio, se me cobrará su sustitución.
- No desprestigiaré el nombre del colegio; comprobaré mis correos del colegio con regularidad para poder trabajar y aprender de forma efectiva.
- Seguiré las normas del colegio sobre honradez académica y no copiaré.

## Política de Seguridad Digital

---

- Sé que si tengo alguna duda tecnológica fuera del colegio puedo pedir ayuda o consejo a mis profesores.
- No intentaré piratear ni ignoraré ningún tipo de seguridad en el hardware o el software que el departamento o el colegio haya instalado.
- No visitaré las páginas o aplicaciones de redes sociales tales como Facebook, Twitter, Instagram o Snapchat mientras esté en clase. Tampoco publicaré cosas hirientes, ofensivas o discriminatorias en las redes sociales ni mientras esté en el colegio ni cuando esté fuera.
- No utilizaré ningún dispositivo para copiar, lo cual incluye el envío de mensajes o uso de internet para encontrar las respuestas de exámenes.
- Entregaré mi dispositivo a los profesores cuando me lo soliciten.
- Comunicaré cualquier caso de ciberacoso de inmediato, tanto si me afecta a mí como a otros, a profesores o a empleados.

He leído los anteriores puntos sobre el uso de dispositivos propios y me comprometo a cumplirlos. Entiendo que si incumplo o hago un mal uso de las normas, el colegio tiene derecho a retirarme el privilegio de utilizar un dispositivo en el colegio. He leído el acuerdo sobre seguridad digital y me comprometo a cumplirlo. Entiendo que si incumplo las normas en él contenidas o en el acuerdo sobre el uso de dispositivos propios, tendré que asumir la sanción correspondiente, que podría incluir la pérdida de acceso a la red del colegio y/o internet, un aviso a los padres/tutores y la pérdida del permiso para traer un dispositivo a clase.

Entiendo que todas las imágenes digitales y/o nombres, direcciones, direcciones de correo electrónico, números de teléfono o los datos personales de los alumnos y empleados que se encuentren en mi dispositivo se consideran datos personales y, como tales, están sujetos a la legislación de protección de datos, es decir el RGPD 2016 (y sus modificaciones y extensiones). Me comprometo a no usar ni compartir esas imágenes de manera alguna sin consentimiento previo por escrito.

Nombre del alumno.....

Firma .....

Fecha .....

### Anexo 7 – Protocolo sobre correo electrónico

#### Prácticas de excelencia en correos electrónicos

- Escriba correos bien estructurados y añada asuntos breves y descriptivos.
- Las frases deberían ser breves y concisas. Puede comenzar el correo con “Hola” o “Estimado”, y el nombre de la persona. El uso de abreviaturas y caracteres de internet tales como los emoticonos no es recomendable.
- La firma debe incluir su nombre, su cargo y el nombre del colegio. Se debe añadir una declaración legal debajo de la firma.
- Los usuarios deben comprobar que el correo no contenga errores ortográficos antes de enviarlo.
- Solo marque los correos como importantes si de verdad lo son.
- Evite enviar cadenas largas de mensajes; comience conversaciones nuevas.

#### NO

- Escriba nada en un correo electrónico si no fuera capaz de escribirlo en un tablón de anuncios de la oficina o en un periódico.
- Escriba nada injurioso, difamatorio, ofensivo, racista u obsceno; se podrá responsabilizar al colegio o a usted mismo.
- Divulgue información confidencial; se podrá responsabilizar al colegio y a usted mismo.
- Reenvíe un mensaje que contenga información sensible sin haber recibido permiso del emisor primero.
- Envíe correos electrónicos usando la cuenta de otra persona.

## Política de Seguridad Digital

---

<b>Propiedad y Consulta</b>	
Redactor (cargo)	Director de Educación
Autor	James Carroll, ADE
Consulta - mayo de 2017	Consulta con: Colchester High School, Cumnor Girls' School, El Limonar Villamartin, North Bridge House Nursery and Pre-Prep School, Oxford House School, Southbank International School Kensington and Hampstead Campus, St Clare's School and St Nicholas Prep School. Representante equipo educativo – Karen Nicholson, ADE.
Actualizada – mayo 2018	Andy Perryer, Digital Learning Adviser

<b>Destinatarios</b>	
Destinatarios	Todo el personal del colegio

<b>Aplicación del documento</b>	
Inglaterra	Sí
Gales	Sí
España	Sí

<b>Control Versión</b>	
Fecha Implementación	01.09.2018
Fecha revision	Revisión para implementación septiembre 2019

<b>Documentación relacionada</b>	
Documentación relacionada	Safeguarding and Child Protection Policy Preventing Radicalisation and Extremism Policy Behaviour Policy