Política de Seguridad y Uso Adecuado y Acordado en el uso de las Nuevas Tecnologías por parte del Alumnado

Creemos que las TIC tienen un papel fundamental en la preparación de los estudiantes para la vida en el siglo XXI y que las TIC pueden tener un impacto positivo en la enseñanza y el aprendizaje. El uso efectivo de estas tecnologías requiere conocer los beneficios y los riesgos, el desarrollo de nuevas habilidades y la comprensión de su uso apropiado y efectivo tanto dentro como fuera del aula. Este documento de política ha sido elaborado para proteger a todas las partes - los estudiantes, el personal y la escuela - y tiene por objeto proporcionar asesoramiento y orientación claros sobre cómo minimizar los riesgos y cómo hacer frente a cualquier infracción.

Para garantizar la seguridad y la confidencialidad

- Todos los estudiantes deben mantener la seguridad de la contraseña en la red. Las contraseñas no deben ser escritas ni compartidas con otros estudiantes. Los profesores de la clase tendrán una copia de las contraseñas y nombres de usuario del alumnado que guardará en un armario cerrado con llave.

- Los dispositivos de almacenamiento de datos (bolígrafos USB, discos duros portátiles, CD ROM y DVD ROM) deben estar sujetos a medidas de protección antivirus mediante la "detención" de los dispositivos antes de su extracción del ordenador, y no deben insertarse en primer lugar si no se puede confiar en la fuente. Los lápices USB deben limpiarse antes de usarlos en los ordenadores o portátiles del centro educativo. Como medida preventiva, los bolígrafos USB del alumnado de KS3 no pueden llevarse nunca a casa, deben permanecer siempre en el colegio.

- Los profesores deben controlar el uso de los iPads del alumnado durante las lecciones.

- Cualquier acceso accidental a material inapropiado en Internet debe ser inmediatamente comunicado a la directora académica del colegio. El

centro educativo se reserva el derecho de examinar los registros de acceso a Internet desde cualquier ordenador o iPad de la escuela. El colegio no puede aceptar la responsabilidad por el material al que se acceda ni las consecuencias del acceso a Internet.

Para Salvaguardar a los Niños

El Libro Verde, "Cada niño es importante", junto con las disposiciones de la Ley de la Infancia de 2004, Keeping Children Safe in Education 2018 y el documento de política Working Together to Safeguard Children 2018 (Trabajando juntos para salvaguardar a los niños en 2018), establece la forma en que las organizaciones y los individuos deben trabajar juntos para salvaguardar y promover el bienestar de los niños.

El resultado de "estar seguros" incluye los objetivos de que nuestros niños y jóvenes estén:

- A salvo de malos tratos, negligencia, violencia y explotación sexual
- A salvo de lesiones accidentales y fallecimiento
- A salvo de acoso y discriminación
- A salvo de la delincuencia y del comportamiento antisocial dentro y fuera de la escuela
- Seguro, estable y protegido.

Estos objetivos se aplican igualmente al "mundo virtual" que los niños y jóvenes encontrarán cuando utilicen las TIC en sus diversas formas. Por ejemplo, es necesario proteger a los alumnos de peligros como:

- El uso de Internet para la captación de niños y jóvenes con el objetivo último de explotarlos sexualmente.

- El uso de las TIC como una nueva arma para los acosadores, que pueden atormentar a sus víctimas a través de sitios web, mensajes de texto o estar expuesto a contenidos inapropiados online, lo que a veces puede conducir a su implicación en delitos y comportamientos antisociales.

Para concienciar a nuestros alumnos de estos peligros, las clases de PSHEE incluirá la enseñanza de actividades online como el grooming y el sexting y la discusión sobre el ciberacoso, sus características, sus efectos en las

víctimas y las sanciones por parte de la escuela. En KS4 y 6th Form, se organizarán sesiones de formación para alertar a los estudiantes sobre estas formas de abuso y la tolerancia cero del BST a las mismas.

En el BST somos conocedores de que los niños con necesidades educativas especiales (SEND) o con alguna discapacidad son particularmente vulnerables al abuso online y, por esta razón, nos esforzamos para asegurarnos de que cada miembro del personal trabaje para ayudar a estos niños a sentirse parte de la comunidad escolar y así aumentar su resistencia/recuperación a cualquier forma de maltrato/abuso/acoso.

Se invita a los cuerpos de seguridad del estado a nuestro centro educato para que impartan formación adicional sobre seguridad online a los niños en Year 7, seg´n el marco de disposición local de seguridad online para los niños en edad escolar de la isla.

Como la radicalización y el extremismo también se llevan a cabo online, todos los miembros del personal asistirá a un curso de formación sobre este tema impartido por la Policía Nacional.

Junto con estos pasos para ayudar a proteger a los niños, el centro educativo cuenta con un sistema de filtrado web para evitar que el alumnado vea contenido inapropiado.

En el BST todos nuestros estudiantes saben que pueden dirigirse a cualquier miembro del personal si tienen un problema y que se les escuchará y se tomará en serio su preocupación.

Los padres también reciben información sobre el acoso online, incluyendo las acciones que el centro educativo toma para prevenirlo y el apoyo que se le da a los niños afectados por el mismo.

Para salvaguardar las instalaciones y apoyar el comportamiento del estudiante

-Los estudiantes siempre deben ser supervisados en las aulas de Informática y en las clases donde se utilizan portátiles/ordenadores/iPads.

-Una vez descubiertos, todos los daños deben ser reportados inmediatamente.

-Queda completamente prohibido comer y beber en las aulas de Informática o en las clases en las que se utilicen portátiles.

¿Cómo se procederá con las quejas relacionadas con las nuevas tecnologías?

El centro educativo tomará todas las precauciones razonables para garantizar la seguridad relacionada con las nuevas tecnologías. Sin embargo, debido a la escala internacional y a la naturaleza vinculada de los contenidos de Internet, a la disponibilidad de tecnologías móviles y a la rapidez de los cambios, no es posible garantizar que no pueda aparecer material inadecuado en un ordenador o dispositivo móvil de la escuela.

Sanciones aplicables por un uso inadecuado de los ordenadores:

-Entrevista, asesoramiento y/o medidas disciplinarias por parte del profesor de la clase, del coordinador de las TIC, del profesor de informática o de la directora académica.
-Informar a los padres o cuidadores.
- Eliminación del acceso a Internet o al ordenador/iPad durante un tiempo (lo que podría impedir en última instancia el acceso a los archivos del sistema).
-Suspensión del colegio o expulsion.
-Se informará a la policía o a Asuntos Sociales.

El DSL actuará como primer punto de contacto para cualquier queja.

Cualquier queja sobre el mal uso por parte del personal del equipo informático será elevada a la Directora Académica y al DSL pudiendo abrirse un procedimiento disciplinario formal.

Las quejas de acoso cibernético se tratan de acuerdo con nuestra Política contra el acoso cibernético.

Se revisará en enero de 2020