E-Safety Policy

Política de Ciberseguridad

Review Frequency	Annually
Most Recent Review	Summer 2025
Next Review Due	Summer 2026
Head Teacher	Ricardo Diaz

1 Alcance

1.1 El Colegio se compromete a promover y salvaguardar el bienestar de todos los estudiantes y una estrategia efectiva de seguridad en línea es primordial para esto .

1.2 Los objetivos de la estrategia de seguridad en línea del Colegio son tres:

- Proteger a toda la comunidad escolar de contenido o contacto ilegal, inapropiado y dañino;
- Educar a toda la comunidad escolar sobre su acceso y uso de la tecnología; y
- Establecer mecanismos efectivos para identificar, intervenir y escalar incidentes cuando sea apropiado.

1.3 Al considerar el alcance de la estrategia de seguridad en línea del Colegio, el Colegio adoptará un enfoque amplio y con propósito para considerar lo que entra dentro del significado de tecnología, redes y dispositivos utilizados para ver o intercambiar información, incluida la tecnología de comunicaciones (denominados colectivamente en esta política como Tecnología).

1.4 Esta política se aplica a todos los miembros de la comunidad escolar, incluido el personal y los voluntarios, los estudiantes, los padres y los visitantes, que tienen acceso a la Tecnología del Colegio, ya sea dentro o fuera de las instalaciones del Colegio, o que de otro modo utilicen la Tecnología de una manera que afecte el bienestar de otros estudiantes o cualquier miembro de la comunidad escolar o cuando la cultura o reputación del Colegio se ponga en riesgo.

1.5 Las siguientes políticas, procedimientos y materiales de recursos también son relevantes para las prácticas de seguridad en línea del Colegio:

- Política contra el Acoso (Anti-Bullying Policy)
- Código de Conducta del Personal (Staff Code of Conduct)
- Política de Uso Aceptable para Estudiantes (Acceptable Use Policy for Students)
- Política de Salvaguarda (Safeguarding Policy)

1.6 Estas políticas, procedimientos y materiales de recursos están disponibles para el personal.

1.7 Esta es una política de todo el Colegio.

2 Roles y responsabilidades

2.1 El Propietario/ISP

2.1.1 El propietario tiene la responsabilidad general de los acuerdos de salvaguarda dentro del Colegio, incluido el enfoque del Colegio hacia la seguridad en línea y el uso de la tecnología dentro del Colegio.

2.1.2 Se requiere que el propietario se asegure de que todos aquellos con responsabilidades de liderazgo y gestión en el Colegio promuevan activamente el bienestar de los estudiantes. La adopción de esta política es parte de la respuesta del propietario a este deber.

2.1.3 El propietario llevará a cabo una revisión anual de los procedimientos de salvaguarda del Colegio y su implementación, lo que incluirá la consideración de la efectividad de esta política y las políticas relacionadas para cumplir con los objetivos establecidos en el párrafo 1.2 anterior.

2.2 Director y Equipo de Liderazgo y Gestión Senior

2.2.1 El Director tiene la responsabilidad ejecutiva general de la seguridad y el bienestar de los miembros de la comunidad escolar.

2.2.2 Los Líderes Designados de Salvaguarda (DSL) son miembros senior del personal del Equipo de Liderazgo Senior y Gestión Escolar (SLMT) con responsabilidad principal en materia de salvaguarda y protección infantil. La responsabilidad del DSL incluye la gestión de incidentes de salvaguarda que involucren el uso de Tecnología de la misma manera que otros asuntos de salvaguarda, de acuerdo con la Política de Salvaguarda del Colegio.

2.2.3 Los DSL trabajarán con el Jefe de TIC y el Responsable de IT (ver abajo) en el seguimiento de los usos y prácticas de la Tecnología en todo el Colegio y en la evaluación de si se pueden realizar mejoras para garantizar la seguridad en línea y el bienestar de los estudiantes.

2.2.4 Los DSL supervisarán regularmente el Registro de Incidentes de Tecnología (Technology Incident Log) mantenido por el Responsable de IT.

2.2.5 El DSL actualizará regularmente a otros miembros del SLMT sobre el funcionamiento de los acuerdos de salvaguarda del Colegio, incluidas las prácticas de seguridad en línea.

2.3 Responsable de IT

2.3.1 El Responsable de IT, junto con su equipo, es responsable de la operación efectiva del sistema de filtrado del Colegio para que los estudiantes y el personal no puedan acceder a ningún material que represente un riesgo de salvaguarda, incluido material terrorista y extremista, mientras usan la red del Colegio.

2.3.2 El Responsable de IT es responsable de asegurar que:

(a) la infraestructura de Tecnología del Colegio sea segura y, en la medida de lo posible, no esté abierta a un mal uso o ataque malicioso;

(b) el usuario solo pueda usar la Tecnología del Colegio si está debidamente autenticado y autorizado;

(c) el Colegio tenga una política de filtrado efectiva implementada y que se aplique y actualice de forma regular;

(d) se minimicen los riesgos de que los estudiantes y el personal eludan las salvaguardas implementadas por el Colegio;

(e) el uso de la Tecnología del Colegio se monitoree regularmente para garantizar el cumplimiento de esta política y que cualquier mal uso o intento de mal uso pueda identificarse y reportarse a la persona apropiada para su investigación; y

(f) el software y los sistemas de monitoreo se mantengan actualizados para permitir que el equipo de TIC monitoree el uso del correo electrónico e internet a través de la red del Colegio y mantenga registros de dicho uso.

2.3.3 El Responsable de IT proporcionará detalles a solicitud, describiendo la provisión técnica actual y las salvaguardas implementadas para filtrar y monitorear contenido inapropiado y para alertar al Colegio sobre problemas de salvaguarda. **Seguridad de los dispositivos** Además, todos los dispositivos utilizados por nuestros estudiantes no solo tienen una garantía técnica, sino también sistemas avanzados de seguridad digital y control de contenido para garantizar un entorno de aprendizaje seguro y apropiado. Actualmente, nuestro equipo está protegido por:

- **Fortinet**, que proporciona un sistema de filtrado actualizado y efectivo, garantiza la protección contra contenido inapropiado y amenazas en línea.

- **IMTLazarus**, una plataforma integral que permite la gestión del aula digital, controlando el uso de aplicaciones y el acceso a contenido por parte del estudiante.

- **SmoothWall**, un filtro inteligente que actúa en tiempo real a través de análisis contextual y filtrado de palabras clave, bloqueando el acceso a sitios web inapropiados o potencialmente peligrosos. Con esta combinación de herramientas líderes en la industria, reforzamos nuestro compromiso con el uso responsable, seguro y pedagógicamente supervisado de la tecnología en el aula.

2.3.4 El Responsable de It informará regularmente al SLMT sobre la operación de la Tecnología del Colegio. Si el Responsable de IT tiene inquietudes sobre la funcionalidad, efectividad, idoneidad o uso de la Tecnología dentro del Colegio, las escalará de inmediato a los miembros apropiados del Equipo de Liderazgo Senior del Colegio (SLT).

2.3.5 El Responsable de IT es responsable de mantener el Registro de Incidentes de Tecnología (Technology Incident Log) y de poner cualquier asunto de preocupación de salvaguarda en conocimiento del DSL de acuerdo con la Política y Procedimientos de Protección Infantil y Salvaguarda del Colegio.

2.4 Todo el personal

2.4.1 El personal del Colegio tiene la responsabilidad de actuar como un buen modelo a seguir en su uso de la Tecnología y de compartir su conocimiento de las políticas del Colegio y de las prácticas seguras con los estudiantes.

2.4.2 Se espera que el personal se adhiera, en la medida en que sea aplicable, a cada una de las políticas a las que se hace referencia en el párrafo 1.5 anterior.

2.4.3 El personal tiene la responsabilidad de informar cualquier inquietud sobre el bienestar y la seguridad de un alumno de acuerdo con esta política y la Política de Salvaguarda y Protección Infantil del Colegio.

2.5 Padres

2.5.1 El papel de los padres para garantizar que los estudiantes comprendan cómo mantenerse seguros al usar la Tecnología es crucial. El Colegio espera que los padres promuevan prácticas seguras al usar la Tecnología y:

(a) apoyen al Colegio en la implementación de esta política e informen cualquier inquietud de acuerdo con las políticas y procedimientos del Colegio;

(b) hablen con su hijo para comprender las formas en que están utilizando internet, las redes sociales y sus dispositivos móviles y promuevan un comportamiento responsable; y

(c) animen a su hijo a hablar con alguien si está siendo acosado o está preocupado por su propia seguridad o la de otro alumno o necesita apoyo.

2.5.2 Si los padres tienen alguna inquietud o requieren información sobre seguridad en línea, deben comunicarse con el DSL.

3 Educación y formación

3.1 Estudiantes

3.1.1 El uso seguro de la Tecnología es integral al plan de estudios de TIC del Colegio. Los estudiantes son educados de manera apropiada para su edad sobre la importancia del uso seguro y responsable de la Tecnología, incluido internet, las redes sociales y los dispositivos electrónicos móviles (ver la Política Curricular del Colegio).

3.1.2 La Tecnología se incluye en los programas educativos seguidos en el EYFS (Etapa de Fundación de la Primera Infancia) de las siguientes maneras:

(a) se guía a los niños para que den sentido a su mundo físico y a su comunidad a través de oportunidades para explorar, observar y aprender sobre personas, lugares, tecnología y el medio ambiente;

(b) se permite a los niños explorar y jugar con una amplia gama de medios y materiales y se les proporciona oportunidades y estímulo para compartir sus pensamientos, ideas y sentimientos a través de una variedad de actividades en arte, música, movimiento, danza, juegos de rol y diseño y tecnología; y

(c) se guía a los niños para que reconozcan que se utiliza una variedad de tecnología en lugares como hogares y Colegios y se les anima a seleccionar y usar la tecnología para propósitos particulares.

3.1.3 El uso seguro de la Tecnología también es un foco en todas las áreas del plan de estudios y los mensajes clave de seguridad se refuerzan como parte de las asambleas y actividades tutoriales/pastorales, enseñando a los estudiantes:

(a) sobre los riesgos asociados con el uso de la Tecnología y cómo protegerse a sí mismos y a sus compañeros de los riesgos potenciales;

(b) a ser críticamente conscientes del contenido al que acceden en línea y se les guía para validar la precisión de la información;

(c) cómo reconocer comportamientos sospechosos, de acoso, de radicalización y extremistas;

(d) la definición de ciberacoso, sus efectos en la víctima y cómo tratar las identidades en línea de los demás con respeto;

(e) las consecuencias del comportamiento negativo en línea; y

(f) cómo reportar el ciberacoso y/o incidentes que hacen que los estudiantes se sientan incómodos o amenazados y cómo el Colegio tratará con aquellos que se comportan mal.

3.1.4 La Política de Uso Aceptable de TIC para Estudiantes del Colegio establece las reglas del Colegio sobre el uso de la Tecnología, incluido internet, correo electrónico, redes sociales y dispositivos electrónicos móviles, ayudando a los estudiantes a protegerse a sí mismos y a otros al usar la Tecnología. Se recuerda a los estudiantes la importancia de esta política de forma regular.

3.2 Personal

3.2.1 El Colegio proporciona formación sobre el uso seguro de la Tecnología al personal para que estén conscientes de cómo proteger a los estudiantes y a sí mismos de los riesgos del uso de la Tecnología y cómo abordar adecuadamente los incidentes que involucran el uso de la Tecnología cuando ocurren.

3.2.2 La formación de inducción para el nuevo personal incluye orientación sobre esta política, así como el Código de Conducta del Personal, la Política de Correo Electrónico e Internet y la Política de Pautas de Uso Profesional de Redes Sociales. La formación continua para el desarrollo del personal incluye formación sobre seguridad tecnológica junto con problemas específicos de salvaguarda, incluido el ciberacoso y la radicalización.

3.2.3 El personal también recibe orientación sobre protección de datos en la inducción y a intervalos regulares posteriores.

3.2.4 La frecuencia, el nivel y el enfoque de toda esta formación dependerán de los roles y requisitos individuales y se proporcionarán como parte del enfoque general de salvaguarda del Colegio.

3.3 Padres

3.3.1 La información está disponible para los padres a través del portal Firefly. Además, ofrecemos la oportunidad para que los padres asistan a sesiones basadas en el Colegio sobre seguridad en línea anualmente.

3.3.2 Se anima a los padres a leer la Política de Uso Aceptable para Estudiantes con su hijo/hija para asegurar que se entienda completamente.

3.4 Recursos útiles

3.4.1 Hay recursos útiles sobre el uso seguro de la Tecnología disponibles a través de varios sitios web, incluyendo:

(a) `http://www.thinkuknow.co.uk/

(b) `https://www.disrespectnobody.co.uk/

(c) `http://www.saferinternet.org.uk/

(d) `https://www.internetmatters.org/

(e) `http://educateagainsthate.com/

(f) `http://www.kidsmart.org.uk/

(g) `http://www.safetynetkids.org.uk/`

(h) `http://www.safekids.com/`

(i) `http://parentinfo.org/`

4 Acceso a la Tecnología del Colegio

4.1 El Colegio proporciona acceso a internet e intranet y un sistema de correo electrónico a estudiantes y personal, así como otra Tecnología. Los estudiantes y el personal deben cumplir con la respectiva Política de Uso Aceptable de la Tecnología al usar la Tecnología del Colegio. Todo ese uso es monitoreado por el Responsable de TI y su equipo.

4.2 Los estudiantes y el personal requieren nombres de usuario y contraseñas individuales para acceder a los sitios de internet e intranet y al sistema de correo electrónico del Colegio, los cuales no deben divulgarse a ninguna otra persona. Cualquier estudiante o miembro del personal que tenga un problema con sus nombres de usuario o contraseñas debe informarlo al Departamento de IT de inmediato.

4.3 No se puede conectar ninguna computadora portátil, tableta u otro dispositivo electrónico móvil a la red del Colegio sin el consentimiento del Responsable de IT. Todos los dispositivos conectados a la red del Colegio deben tener instalado software antivirus actual y actualizado y tener aplicadas las últimas actualizaciones del sistema operativo. El uso de cualquier dispositivo conectado a la red del Colegio será registrado y monitoreado por el Departamento de Soporte de IT.

4.4 El Colegio tiene una conexión Wi-Fi separada disponible para uso de los visitantes del Colegio. Se debe obtener una contraseña, que se cambia regularmente, de un miembro del personal para usar el Wi-Fi. El uso de este servicio será registrado y monitoreado por el Departamento de IT.

4.5 Uso de dispositivos electrónicos móviles

4.5.1 El Colegio tiene sistemas de filtrado y monitoreo apropiados implementados para proteger a los estudiantes que usan Internet (incluidos mensajes de texto por correo electrónico y sitios de redes sociales) cuando están conectados a la red del Colegio. Sin embargo, los dispositivos móviles equipados con una suscripción de datos móviles pueden proporcionar a los estudiantes acceso ilimitado y sin restricciones a internet. Dado que el Colegio no puede establecer una protección adecuada para los estudiantes, no se permite a los estudiantes usar sus dispositivos móviles para conectarse a Internet, incluido el acceso a correo electrónico, mensajes de texto o sitios de redes sociales cuando están bajo el cuidado del Colegio. En ciertas circunstancias, se le puede dar permiso a un estudiante para usar su propio dispositivo móvil para conectarse a Internet utilizando la red del Colegio. El permiso para hacerlo debe solicitarse y otorgarse por adelantado.

4.5.2 Las reglas del Colegio sobre el uso de dispositivos electrónicos móviles se establecen en la Política de Uso Aceptable de la Tecnología para Estudiantes.

4.5.3 El uso de dispositivos electrónicos móviles por parte del personal está cubierto en el Código de Conducta del personal. A menos que se acuerde lo contrario por escrito, los dispositivos móviles personales, incluidos los dispositivos portátiles y *notebook*, no deben usarse para fines del Colegio, excepto en caso de emergencia.

4.5.4 Las políticas del Colegio se aplican al uso de la Tecnología por parte del personal y los estudiantes, ya sea dentro o fuera de las instalaciones del Colegio, y se tomarán las medidas apropiadas cuando dicho uso afecte el bienestar de otros estudiantes o de cualquier miembro de la comunidad escolar o cuando la cultura o reputación del Colegio se ponga en riesgo.

5 Procedimientos para tratar incidentes de mal uso

5.1 Se requiere que el personal, los estudiantes y los padres informen incidentes de mal uso o sospecha de mal uso al Colegio de acuerdo con esta política y las políticas y procedimientos disciplinarios y de salvaguarda del Colegio.

5.2 Mal uso por parte de los estudiantes

5.2.1 Cualquiera que tenga alguna preocupación sobre el mal uso de la Tecnología por parte de los estudiantes debe informarlo para que pueda ser tratado de acuerdo con las políticas de comportamiento y disciplina del Colegio, incluida la Política contra el Acoso (Anti-Bullying Policy) cuando haya una alegación de ciberacoso.

5.2.2 Cualquiera que tenga alguna preocupación sobre el bienestar y la seguridad de un alumno debe informarlo de inmediato de acuerdo con los procedimientos de protección infantil del Colegio (ver la Política de Salvaguarda y Protección Infantil del Colegio).

5.3 Mal uso por parte del personal

5.3.1 Cualquiera que tenga alguna preocupación sobre el mal uso de la Tecnología por parte del personal debe informarlo de acuerdo con la Política de Denuncia de Irregularidades (Whistleblowing Policy) del Colegio para que pueda ser tratado de acuerdo con los procedimientos disciplinarios del personal.

5.3.2 Si alguien tiene una preocupación relacionada con la salvaguarda, debe informarlo de inmediato para que pueda ser tratado de acuerdo con los procedimientos para informar y tratar las alegaciones de abuso contra el personal establecidos en la Política de Salvaguarda y Protección Infantil del Colegio.

5.4 Mal uso por parte de cualquier usuario

5.4.1 Cualquiera que tenga una preocupación sobre el mal uso de la Tecnología por parte de cualquier otro usuario debe informarlo de inmediato al Jefe de TIC o al Director.

5.4.2 El Colegio se reserva el derecho de retirar el acceso a la red del Colegio por parte de cualquier usuario en cualquier momento y de informar de la sospecha de actividad ilegal a la policía.

6 Monitoreo y revisión

6.1 Todos los incidentes graves que involucren el uso de la Tecnología serán registrados centralmente en el Registro de Incidentes de Tecnología (Technology Incident Log) por el Responsable de IT.

6.2 El DSL tiene la responsabilidad de la implementación y revisión de esta política y considerará el registro de incidentes que involucren el uso de la Tecnología y los registros de actividad de internet (incluidos los sitios visitados) como parte del monitoreo continuo de los procedimientos de salvaguarda, para considerar si las prácticas de seguridad existentes y de seguridad en línea dentro del Colegio son adecuadas. La consideración de la efectividad de los procedimientos de seguridad en línea del Colegio y la educación de los estudiantes sobre cómo mantenerse seguros en línea se incluirá en la revisión anual de salvaguarda del SLT.

E-Safety Policy

1 **Scope**

1.1 The School is committed to promoting and safeguarding the welfare of all students and an effective online safety strategy is paramount to this.

1.2 The aims of the School's online safety strategy are threefold:

1. To protect the whole School community from illegal, inappropriate and harmful content or contact;
2. To educate the whole School community about their access to and use of technology; and
3. To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

1.3 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as Technology).

1.4 This policy applies to all members of the School community, including staff and volunteers, students, parents and visitors, who have access to the School's Technology whether on or off School premises, or otherwise use Technology in a way which affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

1.5 The following policies, procedures and resource materials are also relevant to the School's online safety practices:

- Anti-BullyingPolicy
- Staff Code of Conduct
- Acceptable Use Policy for Students

- Safeguarding Policy

1.6 These policies procedures and resource materials are available to staff

1.7 This is a whole School policy

2 Roles and responsibilities

2.1 **The Proprietor /ISP**

2.1.1 The proprietor has overall responsibility for safeguarding arrangements within the School, including the School's approach to online safety and the use of technology within the School.

2.1.2 The proprietor is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of students. The adoption of this policy is part of the proprietors response to this duty .

2.1.3 The proprietor will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in paragraph 1.2 above.

2.2 **Principal and Senior Leadership and Management Team**

2.2.1 The Principal has overall executive responsibility for the safety and welfare of members of the School community.

2.2.2 The Designated Safeguarding Leads (DSL) are senior members of staff from the Senior Leadership and School Management Team (SLMT) with lead responsibility for safeguarding and child protection. The responsibility of the DSL includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding Policy.

2.2.3 The DSLs will work with the Head of ICT and the IT Manager (see below) in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of students.

2.2.4 The DSLs will regularly monitor the Technology Incident Log maintained by the IT Manager.

2.2.5 The DSL will regularly update other members of the SLMT on the operation of the School's safeguarding arrangements, including online safety practices.

2.3 **IT Manager**

2.3.1 The IT Manager, together with his team, is responsible for the effective operation of the School's filtering system so that students and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

2.3.2 The IT Manager is responsible for ensuring that:

(a) the School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

(b) the user may only use the School's Technology if they are properly authenticated and authorised;

(c) the School has an effective filtering policy in place and that it is applied and updated on a regular basis;

(d) the risks of students and staff circumventing the safeguards put in place by the School are minimised;

(e) the use of the School's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(f) monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

2.3.3 The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the School to safeguarding issues.

Device Security

Furthermore, all devices used by our students have not only a technical warranty but also advanced digital security and content control systems to ensure a safe and appropriate learning environment.

Currently, our equipment is protected by:

- **Fortinet**, which provides an up-to-date and effective filtering system, guarantees protection against inappropriate content and online threats.
- **IMTLazarus**, a comprehensive platform that allows digital classroom management, controlling the use of applications and access to content by the student.
- **SmoothWall**, an intelligent filter that acts in real-time through contextual analysis and keyword filtering, blocking access to inappropriate or potentially dangerous websites.

With this combination of industry-leading tools, we reinforce our commitment to responsible, secure, and pedagogically supervised use of technology in the classroom.

2.3.4 The IT Manager will report regularly to the SLMT on the operation of the School's Technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, s/he will escalate those concerns promptly to the appropriate members(s) of the School's Senior Leadership Team (SL T).

2.3.5 The IT Manager is responsible for maintaining the Technology Incident Log and bringing any matters of safeguarding concern to the attention of the DSL in accordance with the School's Child Protection & Safeguarding Policy and Procedures.

2.4 **All staff**

2.4.1 The School staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the students.

2.4.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in paragraph 1.5 above.

2.4.3 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding & Child Protection Policy.

2.5 **Parents**

2.5.1 The role of parents in ensuring that students understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:

(a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

2.5.2 If parents have any concerns or require any information about online safety, they should contact the DSL.

Education and training

3.1 **Students**

3.1.1 The safe use of Technology is integral to the School's ICT curriculum. Students are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices (see the School's Curriculum Policy).

3.1.2 Technology is included in the educational programmes followed in the EYFS in the following ways:

(a) children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

(b) children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

(c) children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use technology for particular purposes.

3.1.3 The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching students

(a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;

(b) to be critically aware of content they access online and guided to validate accuracy of information;

(c) how to recognise suspicious, bullying, radicalisation and extremist behaviour;

(d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

(e) the consequences of negative online behaviour; and

(f) how to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

School's Acceptable Use of ICT Policy for Students sets out the School rules about

3.1.4 The the use Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology. Students are reminded of the importance of this policy on a regular basis.

3.2 **Staff**

3.2.1 The School provides training on the safe use of Technology to staff so that they are aware of how to protect students and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

3.2.2 Induction training for new staff includes guidance on this policy as well as the Staff Code of Conduct, Email & Internet Policy and Professional Use of Social Media Guidelines Policy. Ongoing staff development training includes training on Technology safety together with specific safeguarding issues including cyberbullying and radicalisation.

3.2.3 Staff also receive data protection guidance on induction and at regular intervals afterwards.

3.2.4 Thefrequency,levelandfocusofallsuchtrainingwilldependonindividualrolesand requirements and will be provided as part of the School's overarching approach to safeguarding.

3.3 **Parents**

3.3.1 Information is available to parents via the Firefly portal. Additionally, we offer the opportunity for parents to attend School based sessions on online safety on an annual basis.

3.3.2 Parents are encouraged to read the Acceptable Use Policy for Students with their son/daughter to ensure that it is fully understood.

3.4 **Useful resources**

3.4.1 There are useful resources about the safe use of Technology available via various websites including:

(a) http://www.thinkuknow.co.uk/
(b) https://www.disrespectnobody.co.uk/
(c) http://www.saferinternet.org.uk/
(d) https://www.internetmatters.org/
(e) http://educateagainsthate.com/
(f) http://www.kidsmart.org.uk/
(g) http://www.safetynetkids.org.uk/
(h) http://www.safekids.com/
(i) http://parentinfo.org/

4 **Access to the School's Technology**

4.1 The School provides internet and intranet access and an email system to students and staff as well as other Technology. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the IT Manager and his/her team.

4.2 Students and staff require individual user names and passwords to access the School's internet and intranet sites and email system which must not be disclosed to any other person. Any student or member of staff who has a problem with their user names or passwords must report it to the IT Department immediately.

4.3 No laptop, tablet or other mobile electronic device may be connected to the School network without the consent of the IT Manager. All devices connected to the School's network should have current and up-to-date anti-virus software installed and have the latest OS updates applied. The use

of any device connected to the School's network will be logged and monitored by the IT Support Department.

4.4 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.

4.5 **Use of mobile electronic devices**

4.5.1 The School has appropriate filtering and monitoring systems in place to protect students using the Internet (including email text messaging and social media sites) when connected to the School's

network. Mobile devices equipped with a mobile data subscription can, however, provide students with unlimited and unrestricted access to the internet. Since the School cannot put adequate protection for the students in place, students are not allowed to use their mobile devices to connect to the Internet including accessing email, text messages or social media sites when in the School's care. In certain circumstances, a student may be given permission to use their own mobile device to connect to the Internet using the School's network. Permission to do so must be sought and given in advance.

4.5.2 The School rules about the use of mobile electronic devices are set out in the Acceptable Use of Technology Policy for Students.

4.5.3 The use of mobile electronic devices by staff is covered in the staff Code of Conduct. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

4.5.4 The School's policies apply to the use of Technology by staff and students whether on or off School premises and appropriate action will be taken where such use affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

5 **Procedures for dealing with incidents of misuse**

5.1 Staff, students and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

5.2 **Misuse by students**

5.2.1 Anyone who has any concern about the misuse of Technology by students should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

5.2.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding & Child Protection Policy.

5.3 **Misuse by staff**

5.3.1 Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

5.3.2 If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding & Child Protection Policy.

5.4 **Misuse by any user**

5.4.1 Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Head of ICT or the Principal.

5.4.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

6 **Monitoring and review**

6.1 All serious incidents involving the use of Technology will be logged centrally in the Technology Incident Log by the IT Manager.

6.2 The DSL has responsibility for the implementation and review of this policy and will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the School are adequate.

Consideration of the effectiveness of the School's online safety procedures and the education of students about keeping safe online will be included in the SLT´s annual review of safeguarding.