E-Safety Policy

Date Approval	: 26 October 2022	**Next Review**	: 10 January 2027
Review Cycle	: 24 months	**Scope**	: Whole School
Ownership	: Campus Principal	**Approved by**	: SLT

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:

- To protect the whole School community from illegal, inappropriate, and harmful content or contact.
- To educate the whole School community about their access to and use of technology.
- 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:

Safeguarding Policy
Anti-Bullying Policy
Staff Code of Conduct
Student Code of Conduct/ Behaviour Policy

1.6 These policies, procedures and resource materials are available to staff.

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 proprietor's 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 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) and Deputies 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 and Deputies 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 , Deputies and assigned members in the safeguarding team will regularly monitor the online Incident Log from the platform used to monitor online activities – Smoothwall Monitor. This is also assisted by a group of appointed staff under the safeguarding team.

2.2.5 The DSL will regularly update other members of the SLT 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:

- the School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack.
- the user may only use the School's Technology if they are properly authenticated and authorised.
- the school has an effective filtering policy in place and that it is applied and updated on a regular basis.
- the risks of students and staff circumventing the safeguards put in place by the school are minimised.
- 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
- 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.

2.3.4 The IT Manager will report to the SLT on the operation of the School's Technology or whenever requested. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, the IT manager 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 should report any incident beyond what is captured by Smoothwall 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 available in the school.

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:

- support the school in the implementation of this policy and report any concerns in line with the School's policies and procedures;
- 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
- 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 or Deputies.

3. 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.

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

- 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.

- 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
- 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

- about the risks associated with using the Technology and how to protect themselves and their peers from potential risks.
- to be critically aware of content they access online and guided to validate accuracy of information.
- how to recognise suspicious, bullying, radicalisation and extremist behaviour.
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.
- the consequences of negative online behaviour; and
- 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.

3.1.4 Student Code of Conduct/behaviour policy sets out the school rules about 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 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the school's overarching approach to safeguarding.

3.3 **Parents**

3.3.1 Parents are encouraged to read the student code of conduct with their child to ensure that it is fully understood.

3.3.2 There are useful resources available for parents to further enhance their knowledge about the safe use of Technology; various websites including:

- https://www.cybersecurity.my/
- https://www.internetmatters.org/

- http://educateagainsthate.com/
- http://www.safekids.com/
- 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 IT team.

4.2 Students and staff require individual usernames 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 usernames or passwords must report it to the IT Department immediately.

4.3 No personal 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 Schools has a separate Wi-Fi connection available for use by visitor or personal devices to the school. The self-registration process could be obtained from Admission or IT department to use the visitor Wi-Fi. Personal information provided is to use for logged and monitored by the IT department.

4.5 All school devices will be installed with Smoothwall which is an added values to identify safeguarding concerns. All concerns alerted by Smoothwall will go directly to safeguarding team to evaluate whether the concern is valid or not before taking the next step to address the issue.
Smoothwall plays a significant role in safeguarding staff and students online activities by providing schools with the tools to monitor and manage internet usage effectively.

4.5 Use of mobile electronic devices

4.5.1 The School has appropriate filtering and monitoring systems in place and will continue enhancing the system 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 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 or own mobile data. 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 Student Code of Conduct/Behaviour Policy.

4.5.3 The use of mobile electronic devices by staff is covered in the staff Code of Conduct/ social media Policy/ safeguarding policy. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency or with prior consent from the principal.

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 safeguarding and 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.

5.3.3 Alerts from Smoothwall regarding staff will go directly to Campus Principal and then will address the issue with respective head of school and/or Human Resource department.

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 and IT manager have 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 ISP annual review of safeguarding.

---------- End of Policy ----------