المدرسة الهندية العالمية الخاصة
INTERNATIONAL INDIAN SCHOOL
P.O. BOX 5665, AJMAN, U.A.E | T : +971 67408333 | info@iisajman.org | www.iisajman.org

Cyber Safety & Security Policy -AY 2026-2027

Ratified	April 2018
Amended	April 2026
Next Review Date	March 2027
Policy Type	Cyber Safety & Security Policy
Reference	UAE Cyber Laws & CBSE guidelines
Related Policies	Child Protection Policy, Data Protection Policy, Filtering Policy, Mobile Device Policy, Password Policy, AUP, Social Media Policy, Behaviour Management Policy
Review Frequency	Annually
Committee Responsible	Online Safety Committee
Chair Signature	PRINCIPAL Ms. Qurat Ul Ain

School Mission and Vision

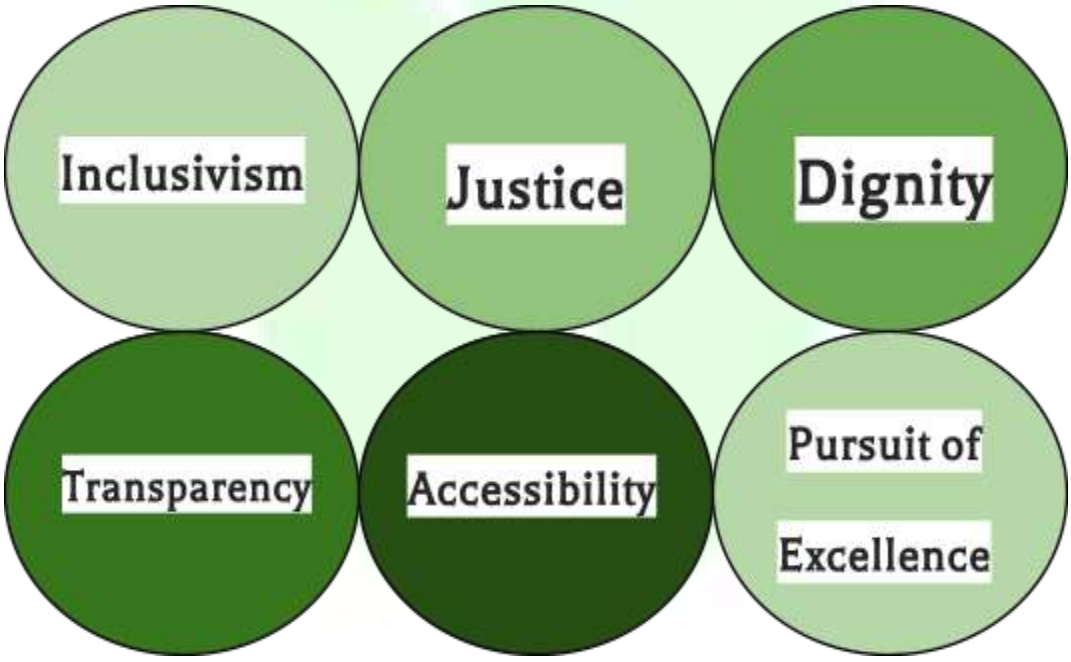
Our Vision

The school envisages learning as a communitarian process of imbibing education from the natural, academic, social and technological ecosystems created around the institution of school.

Our Mission

We strive to provide a new model of education for the expatriate children in the UAE in a culturally inclusive, technologically effective and ecologically sensitive way in a cosmopolitan environment.

CORE VALUES



Members of the committee

- Mr. Wasim Yousuf Bhat (CEO)
- Mr. Qurat al Ain (Principal)
- Mr. Alphin Joby Johnny (Administrative Officer)
- Social Worker
- System Administrator
- System Administrator- Corporate
- Section Heads

Cyber safety and security policy was approved by the Governing body of the school on	2018
The Implementation of this policy will be monitored by the	Online safety group members Student behavior management committee
Monitoring will take place at regular intervals	Annually
Review of the policy	Annually
Next anticipated Review date	March 2027

Abstract: *This document lays down the school Cyber Safety policy on use of online mechanisms and platforms especially in the context of Online Learning. The intention is to make students and parents aware of the best practices and safeguards while using online platforms and make them aware about good online behavior and provide a reliable reporting mechanism in cases a student faces online issues.*

Contents Pages

Introduction:

The Internet, the most interactive technological platform of this century, has become an integral part of our daily lives. It is a learning and communication tool that offers us a wide range of opportunities.
It is an invaluable source of knowledge and encourages creativity and imagination. Internet ethics involves our approach while using it for different purposes. We should be aware that we should always be honest and respect the rights and property of others on the web.

Cyber safety is the safe and responsible use of information and communication technology. It is not just about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette). This policy applies to all members of the school (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.The cyber safety and security policy is interlinked with the School Behavior Management Policy, Health and Safety Policy, Child Protection Policy and IT policy.

Objectives:

● To enable the students, staff and parents to browse the internet safely and understand the importance of using secure connections.

● Inform the students and parents on the protective and safety measures in their use of technology, to be aware of Cyber Bullying.

● To improve awareness of intelligent usage of social media websites and smart usage of educational websites.

● To communicate the etiquettes of electronic communication.

The DO's in the use of Online Technology and Electronic Communication for students:

● Respect the privacy of others.

● Report and flag content that is abusive or illegal.

● Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.

● Report online bullying immediately to the teacher and parents/ or someone whom you trust.

● Use a strong and unique password with combinations of numbers, uppercase and lowercase letter and special characters for each account(s).

● Keep the browser, operating system and antivirus up-to-date.

● Obtain software from trusted sources. Always scan files before opening them.

● Lock your screen when you're finished using your computer/ tablet/ phone. Further, set it to lock automatically when it goes to sleep.

● Check to see if the web address begins with https:// whenever you sign in online.

● Make privacy settings in social media accounts in such a way that profile and posts are visible only to close friends and acquaintances.

● Connect only with known individuals.

● Be mindful of your digital reputation - think twice before you post something embarrassing, harmful or inappropriate.

● Report to the service provider immediately if the account is hacked. If possible deactivate your Account.

The DONT's in the use of Technology and Electronic Communication:

● Don’t share your mobile number or parent’s mobile number.

● Don’t share your address/location.

● Don't share your personal information: real name, date of birth, etc. unnecessarily.

● Don’t share bank account numbers or credit card numbers of your parents.

● Don’t share your Social Security number /Emirates ID.

● Don’t share your Passwords.

● Don't send your pictures to unknown persons or share them on social media.

● Don't open emails and attachments from strangers.

● Don't respond to any suspicious email, instant message or web page asking for personal Information.

● Don't enter a password when someone is sitting beside you as they may see it.

● Don't save your username and password on the browser.

● Don't steal other's information.

● Don't access or use files without the permission of the owner.

● Don't copy software which has copyright without the author's permission.

● Don't bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.

● Don't use someone else's password even if it is shared with you.

● Don't log in as someone else to read their emails or mess with their online profiles.

● Don't attempt to infect or in any way try to make someone else's computer unusable.

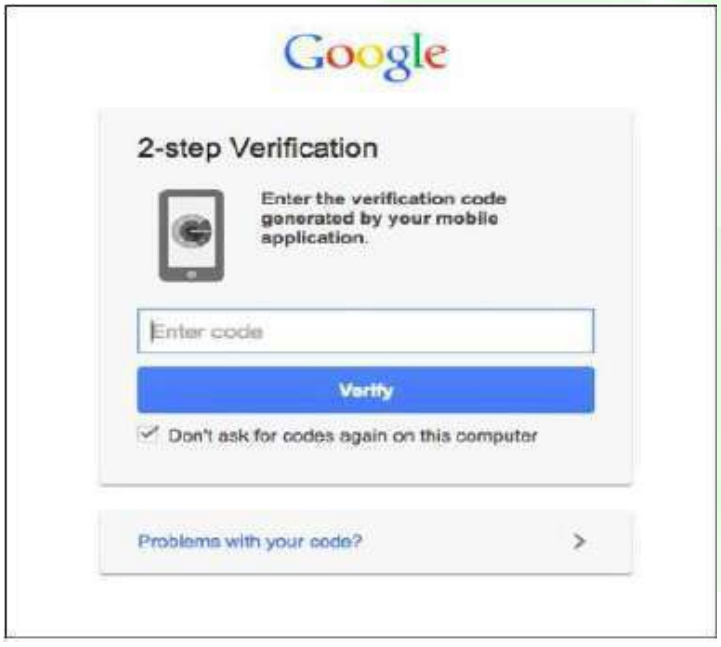
● Don't meet unknown (even if they are known only through online interaction) people alone; always inform your parent.

● Don't open or download any attachments from an unknown source as they may contain viruses.

Tips for safe internet browsing

1. Update your browser frequently

2. Turn on Two-Factor Authentication whenever possible. Most of the websites critical to our lives (online banking websites, Gmail, Facebook etc.) offer two-factor authentication.



3. Customize your security settings. You can also make a browser more secure by customizing it through its preferences or settings menu.

4. Confirming site's security (https vs http) Check for the Secure as shown on the address bar (Chrome).

5. Backup your data. This means finding a way to copy your information to a safe place so that you don't rely on your computer's hard disk alone.

6. Avoid clicking on links if possible from messages or chats. Viruses spread easily through links in instant messages and email attachments.

7. Bookmark important sites If there are sites you visit regularly, it's a good idea to bookmark them in your browser. Bookmarked addresses take you to the same site every time.

Cyber Safety Challenges - Related Terms

• **Cybercrimes** are offences that may be committed against individuals, companies or institutions by using computers, internet or mobile technology. Cybercriminals use platforms such as social networking sites, emails, chat rooms, pirated software, websites, etc., to attack victims. Children are also vulnerable to various types of cybercrimes.

• **Cyber Grooming** is growing as one of the major cyber threats faced by children and teenagers. It is a practice where someone builds an emotional bond with children through social media or messaging platforms with an objective of gaining their trust for sexually abusing or exploiting them. The cyber groomers can use gaming websites, social media, email, chat rooms, instant messaging, etc. by creating a fake account and pretending to be a child or having the same interests as the child.

• **Cyber bullying** means using internet or mobile technology to intentionally harass or bully someone by sending rude, mean or hurtful messages, comments and

images/videos. A cyber bully can use text messages, emails, social media platforms, web pages, chat rooms, etc. to bully others.

The school has a zero tolerance policy for incidents of Cyber Bullying and will take actions as per the national guidelines and laws in case such incidents occur and are reported.

Consequences of Cyber bullying

It can lead to both civil and criminal cases.

CIVIL LAWS

- Defamation.
- Invasion of privacy/public disclosure of a private fact.
- Intentional infliction of emotional distress.

CRIMINAL LAWS

- Criminal laws can lead to the arrest and offenders can be put in jail and get fines as well. Using the internet for the following purposes will attract criminal cases in many countries.

- Hate or bias crimes.

- Making violent threats to people or their property.

- Engaging in coercion. Trying to force someone to do something they don't want to do.

- Making harassing telephone calls, sending obscene text messages, and stalking.

- Sexual exploitation and sending sexual images of children under 18 years of age.

● Taking a photo of someone in a place where privacy is expected (locker room, bathroom, etc.) and exploiting it on the internet.

● Taking a photo of someone without their consent and posting publicly.

If you feel that you are being Cyber Bullied

● Ignore.

● Tell someone.

● Just let a trusted adult know what's going on. The worst thing you can do is to keep it to yourself. Remember, it's not your fault!

● Do not instigate.

● If someone is sending you hurtful messages or posting mean pictures, they're doing it to get an emotional response from you. Don't give them one! Don't respond OR retaliate. This will only encourage them to take it further.

● Block them. If it's on Facebook or another website that allows you to block the person or leave the chat room, then do it!

● Be open to parents about your online identity and image.

● Tell your parents what you do online in general.

● Never indulge in cyber bullying yourself.

How Can I Use Cyber Platforms Safely?

✔ Follow the cyber safety guidelines properly.
✔ Safeguard your device and online accounts.
✔ Don't involve in any kind of improper cyber behavior, even for fun.
✔ If you face any challenge online, immediately inform your parent or elders so that they can support you and contact school if needed.
✔ Always maintain cyber etiquettes while using technology.
✔ Make a note that cybercrimes are punishable offenses; especially the UAE has very strict and stringent laws to deal with Cyber offences.

REPORTING

If a student faces an uncomfortable situation online, specifically if someone is threatening or bullying online, especially during Online Learning sessions, who should be contacted?

Student can directly contact School online safety leader: Ms. Aswani, the social worker
Contact No: 0525956445
Email id: osl@iisajman.org

Other Contacts

Name: Aashiya, KG section in Head, Email Id: kgsection@iisajman.org

Contact No : 0553724853

Ms. Jagrita, Primary 2 section head, Email Id: primary2@iisajman.org

Contact No:0563547884

Ms. Vinu, Girls section section head, E mail Id: girlssection@iisajman.org

Contact No: 0563547912

Mr. Jayakrishnan Boys section section head, Email Id: boyssection@iisajman.org

Contact No: 0502004692

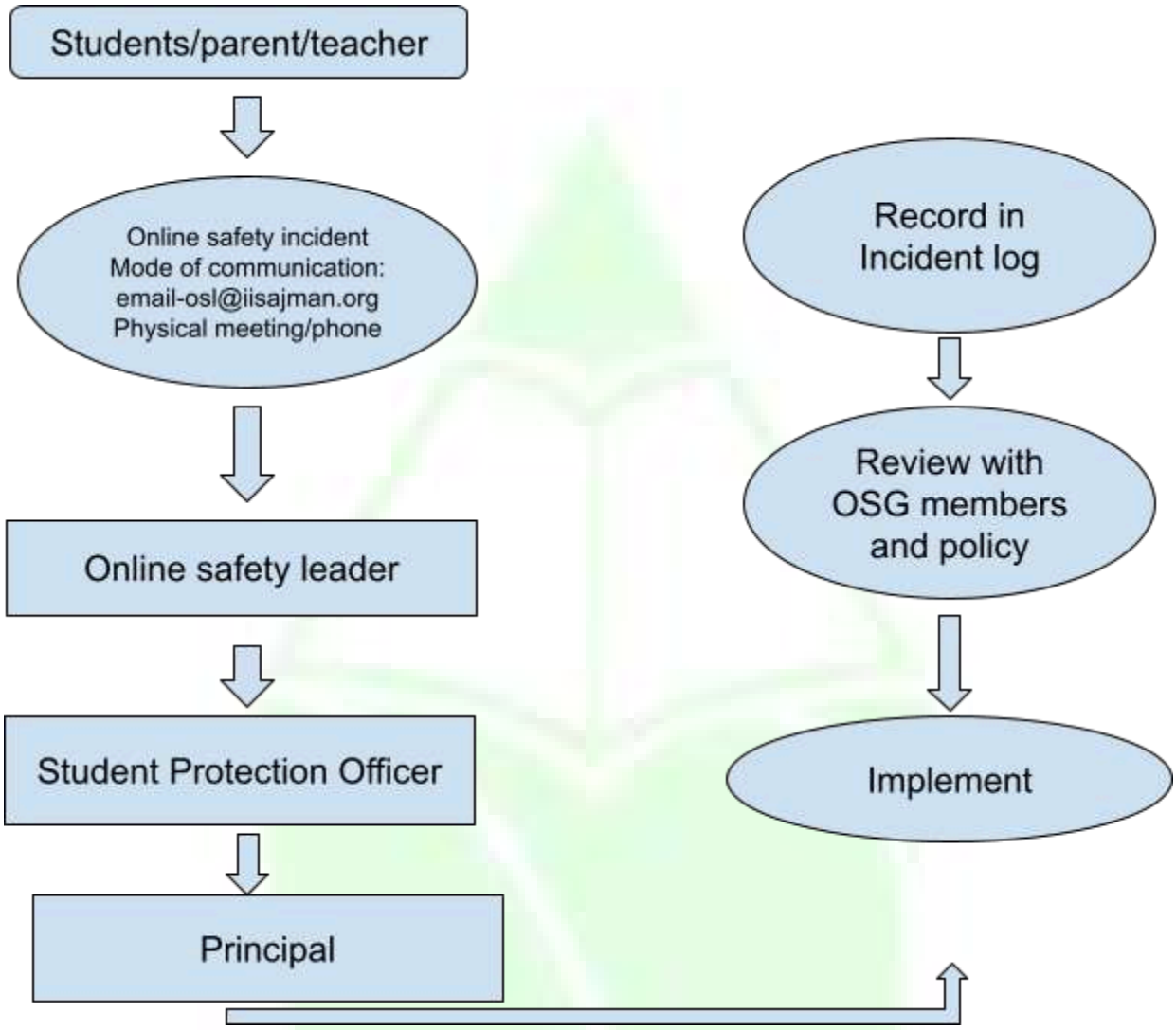
Ms. Qurat Ul Ain , the principal , Child protection officer, Email Id: principal@iisajman.org

Contact No: 0558403796

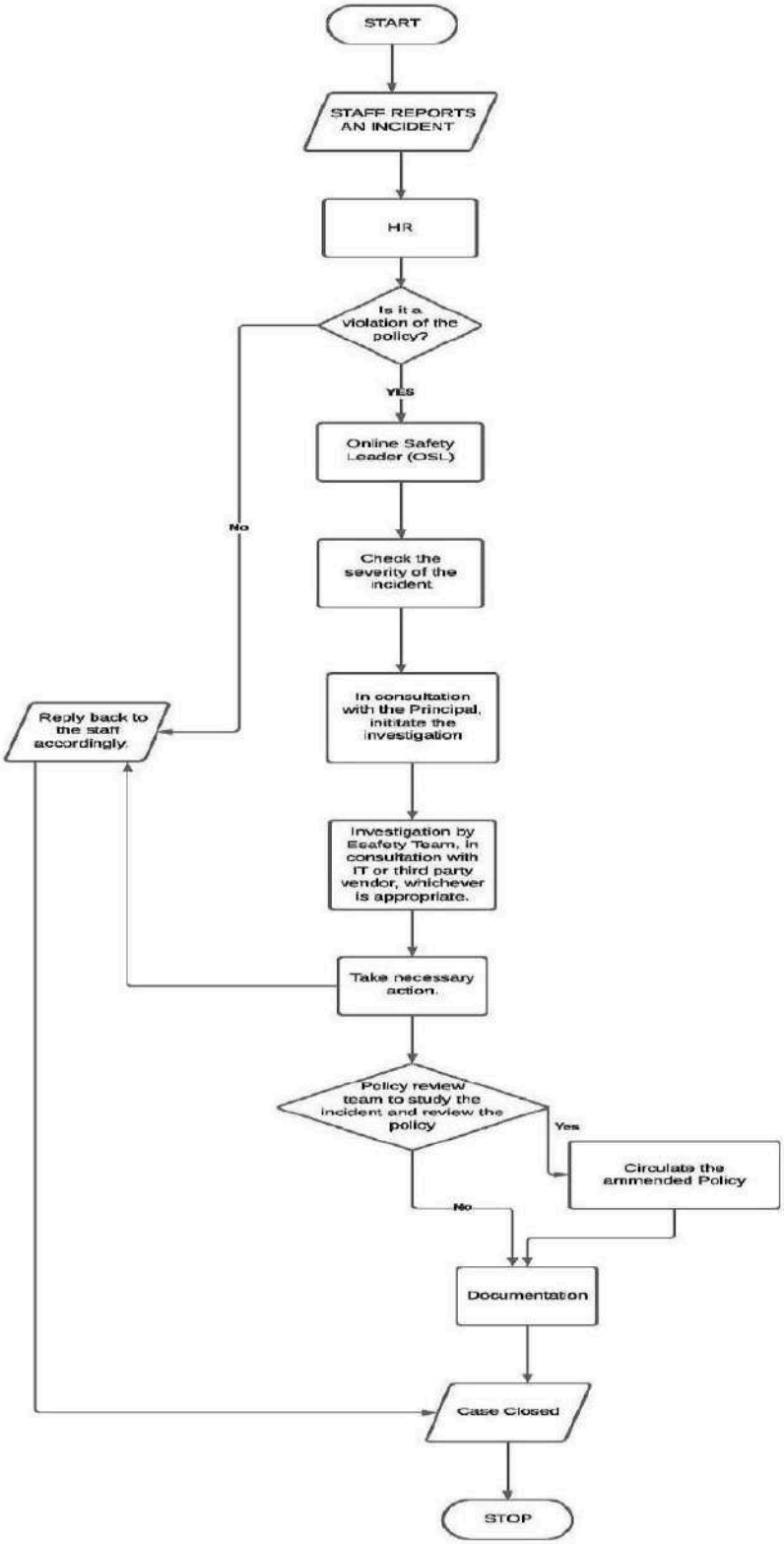
Name: Ms. Diana Yash , Primary 1 section Head, Email id primary1@iisajman.org

Contact No: 0563547882

Reporting procedure for student related online incidents:



Online safety reporting procedure for staff



ROLES AND RESPONSIBILITIES

ONLINE SAFETY GROUP

Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring of the online safety policy including the impact of initiatives.

Membership

The online safety group consist of the following members:-

- Governor
- Student protection officer
- Online Safety Leader
- Senior Leaders (Supervisors)
- ICT Technical Staff
- Teaching staff members
- Parent Council representatives
- Student representatives
- Support staff members

Online Safety Group and Responsibilities

Governor	Mr. Wasim Yousuf , Dean AI
Principal	Ms. Qurat Ul Ain
Vice Principal	Mr. Manzar Alam
Student protection officer	Ms. Sudheesha Rahul
Online safety Leader	Ms. Aswani, Social Worker
Senior Leader (Section heads)	Ms. Jagrita, Ms. Diana Ms. Syeda Asra Ms. Vinu & Mr. Jayakrishnan
Tech Support	Ms. Reshma A, Software Analyst Mr. Manu, System Admin
Teachers' Representative	Ms.Vijitha - KG Ms. Sandya - primary 1 Ms. Vineetha - primary 2 Ms. Rajeswary Alakkal - girls section Ms. Shiyana - boys section
Parents' Representative	Mr. Mansoor Babu- Innovation Parent Ambassador, Ms. Anees Fathima- Safeguarding Parent Ambassador Ms. Sandhya Suresh- Wellbeing Parent Ambassador
Student' Representative	Esafety Ambassadors and Wellness Ambassadors
Supporting Staff	Ms. Conchita

- Other people may be invited to attend the meetings at the request of the Online Safety Head on behalf of the committee to provide advice and assistance where necessary.

- Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

Governor

- ➢ To independently chair the group, ensure minutes are taken and actions are delegated and actioned.

- ➢ Ensure that all initiatives, action points, concerns etc. are raised at Governors meetings.

Principal

➢ The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Leader

 Regular meetings with the E Safety Leader/ E Safety Group.

 Regular updates on the monitoring of E safety incident logs.

 Regular updates on the monitoring of websites.

➢ Inviting other people to attend meetings when required by the committee and guiding the meeting according to the agenda and time available;

➢ Ensuring all discussion items end with a decision, action or definite outcome;

➢ Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

 Plan & provide training for OSL (Online Safety Leader), OSG (Online Safety Group) and associated staff.

 Planning orientation for the staff in order to raise awareness about the policies and its implementation

Online Safety Leader

The Committee has selected Social Worker as the Online Safety Leader (OSL). OSL will be taking day to day responsibilities for E-Safety issues and having a leading role in establishing and reviewing the school E-Safety policies/documents.

Responsibilities of Online Safety Leader

 Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.

 Providing training and advice for staff and parents (along with the Head/Deputy)

 Liaising with the schools Senior Leaders to ensure all school data and information is kept safe and secure

 Liaising with school ICT technical staff and/or school contact from the managed service Provider

 Receiving reports of E-Safety incidents and creating a log of incidents to inform future ESafety developments

 Attending relevant meetings

 Establish a E-safe school culture in wider community

 Empower students and staff by providing appropriate information regarding online safety and training to perform safely.

 Ensure the E- safe school management system continually improved.

 Responsible person for handling the sensitive issues effectively.

 Implement and maintain an E safety program in the wider community.

 Record online safety incidents and actions taken, in accordance with the school's normal child protection mechanisms.

Vice Principal

➢ Support the Principal in ensuring the effective implementation of the school's online safety (E-Safety) policy and procedures.

➢ Oversee the day-to-day monitoring of E-Safety practices across different sections of the school.

➢ Coordinate with the Online Safety Leader (OSL) to review incident reports and ensure appropriate follow-up actions are taken.

➢ Ensure that all staff adhere to E-Safety protocols and report any concerns promptly.

➢ Assist in organizing and monitoring training sessions, awareness programs, and workshops related to cyber safety for staff and students.

➢ Supervise the integration of online safety practices into teaching and learning processes.

➢ Act as a point of escalation for serious E-Safety incidents and support decision-making in line with school policies.

➢ Monitor the effectiveness of E-Safety measures and provide feedback for continuous improvement.

➢ Ensure communication with parents regarding significant E-Safety concerns when required.

Student Protection Officer

➢ Promote awareness of online safety among students through campaigns, assemblies, and peer-led activities.

➢ Encourage responsible and respectful online behavior among students.

➢ Work closely with the Online Safety Leader to support student engagement in E-Safety initiatives.

➢ Identify and report any cyber safety concerns or incidents raised by students to the appropriate authority.

➢ Support the organization of student workshops, seminars, and activities related to digital well-being and cyber safety.

➢ Act as a bridge between students and school authorities in matters related to online safety.

➢ Encourage students to speak up about online risks such as cyberbullying, misuse of social media, or unsafe digital practices.

➢ Assist in developing a student-led E-Safety culture within the school.

➢ Ensure that student prefects/model leaders demonstrate positive digital citizenship at all times.

Senior Leaders (Supervisors)

The Committee has selected Supervisors as the Senior Leaders. The Senior Leaders will be responsible for ensuring the safety (including E-Safety) of members of the school community.
The Senior Leaders are responsible for reporting security incidents as outlined in the school E-Safety Policy. The day to day responsibility for E-Safety will be delegated to all staff who work with students of their respective Sections.

Responsibilities of Senior Leader

 The Senior Leaders are responsible for ensuring that the relevant staff are receiving suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.

 They are also responsible for ensuring that students are taught through orientation session on how to use ICT tools such as the internet, email and social networking sites, safely and appropriately.

 The Senior Leaders will ensure the reporting mechanism to be followed for students and staff for all incidents which fall under Online Safety.

 The Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

 The Senior Leaders will receive regular monitoring reports from the E-Safety Leader.

 The Senior Leaders should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff/student.

 The Senior Leaders are responsible for ensuring that parents, when given access to data and information relating to their child/children via the learning platform, have adequate information and guidance relating to the safe and appropriate use of this online facility.

Tech Support

The Committee has nominated Software Analyst & IT Administrator as Tech Support.

Responsibilities of Tech Support

 Overall monitoring, surveillance and investigative activities which are unsuitable and Inappropriate.

Teachers' Representatives

The Committee has selected 4 teacher representatives who will be responsible to focus on all the areas of curriculum.

Responsibilities of teachers' representatives

 Organizes activities where students can use skills and knowledge in the field of technology which caters online safety education and organizes online safety campaigns.

Parents' Representatives

The Committee has selected Parents' Council members as Parents' representatives.

Responsibilities of parent representatives

- Maintains good communication between parents and teachers
- Ensures the participation in online safety group meeting/orientation
- Ensures the contribution for school decision making process

Students' Representatives

The Committee has selected 4 students as the students' representatives.

Responsibilities of student representatives

- Shows responsibility to report hidden online safety issues among students as per the reporting mechanism of the school.
- Ensures the participation in online safety group meeting
- Awareness of all school policies relating to online safety
- Communicate new ideas and concept with E Safe groups
- Maintain confidentiality of any sensitive issues shared

Supporting Staff

The Committee has appointed 1 Supporting staff.

Responsibilities of Supporting Staff

- Responsible to have an up-to-date awareness of E Safety matters and train the other supporting staff.

Students

Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy and behavioural management policy

- ➢ Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ➢ Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- ➢ Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyberbullying.
- ➢ Should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents

Parents / Caregivers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

Parents are followed when using the school digital technology systems in accordance with the Acceptable Use Policy guidelines and guide the children appropriately.

Parents and caregivers will be encouraged to support the school in promoting good e safety practices.

Education – students

There is a planned and progressive E-Safety awareness delivered throughout the school. Learning opportunities are embedded into the curriculum and shared through assemblies, orientations, activities throughout the school and are taught in all year groups.

E-Safety education is provided in the following ways:

- A planned E-Safety/E-literacy programme will be provided as part of ICT in LMS – this includes the use of ICT and new technologies in school and outside school.

- Key E-Safety messages are reinforced as part of a planned programme of LMS and modules/ pastoral activities.

- Students are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Students are aware of the Student AUP and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Students are taught the importance of information security and the need to keep information such as their password safe and secure

- Staff act as good role models in their use of ICT, the internet, mobile devices and LMS.

Education – parents

The school provides information and awareness to parents through:

- Circulars, official mail & SMS
- Newsletters, web site, Learning Management System, Orisson portal
- Parents session/orientation/meeting and National Online safety platform

Education & Training – Staff

All staff receive regular E-Safety orientation and awareness programs and understand their responsibilities, as outlined in this policy. Further trainings will be offered as follows:

- A planned programme of formal E-Safety training will be made available to staff for the new academic year in collaboration with NOS. It is expected that OSL will identify E-Safety as a training need within the performance management process.

- All new staff will receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies

- This E-Safety policy and its updates are presented to and discussed with staff.

- All staff require training through the National Online safety platform.

- The E safety Leader provides advice / guidance / training as required to individuals.

Training – OSL & OSG

Take part in E-Safety awareness sessions:

This is offered by:

· Participation in school training In House/External sessions for staff or parents.

Curriculum

E-Safety is a focus in all areas of the curriculum and staff re-enforce E-Safety messages in the use of ICT across the curriculum.

- In lessons, where internet use is pre-planned, students are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches.

- Where students are allowed to freely search the internet, e.g. using search engines, staff should monitor the content of the websites the young people visit.

- The school provides opportunities within a range of curriculum areas to teach about E-Safety through LMS as well as Wings curriculum.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request the Tech Support to temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged.

- Students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.

- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies