THE NEW INDIAN SCHOOL

2021

# E-SAFETY POLICY

This draft delineates in detail as how to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.

## Acknowledgement

| | |
|---|---|
| This e-safety policy was approved by the Governing Body on: | February 25, 2021 |
| The implementation of this e-safety policy will be monitored by the: | SLT |
| Monitoring will take place at regular intervals: | Annually |
| The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals: | Annually |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | December 2021 |
| Should serious e-safety incidents take place, the following external persons/agencies should be informed: | RafeeqRahim (Principal)<br>Shakib Ahmed (CEO)<br>Mary Brigeet (Vice Principal) |

**INTRODUCTION:**

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 covers all aspects of the technology usage of students with reference to school context both inside the school premises and in case of Online Learning too. The cyber safety and security policy is interlinked with the School Behavior Management Policy, Health and Safety Policy, Child Protection Policy and IT policy.

**RATIONALE**

The New Indian School UAQ embraces the presence and use of Information and Communication Technologies (ICT) as an integral part of the learning environment. The Internet allows for access to information 24 hours a day, 7 days a week. For school online capabilities not only create entrée to a vast amount of resources but also facilitate distance learning and collaboration between classes and students in different locations. Along with the benefits the Internet brings, however, come costs such as new threats to students. The Cyber Safety policy seeks to ensure the safe and responsible use of ICT within the NIS community.

**OBJECTIVES:**

- To enable the students 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.

**IMPLEMENTATION:**

- The New Indian School promotes partnership between all members of the school community in adhering to this policy. Our approach to cyber safety aligns with our school values and is supported by our ICT Acceptable Use Policy, Digital Media Policy, Virtual Learning Policy and Well-Being Policy.
- Also the school will be strictly following the guidelines of Child Digital Safety policies under the Cyber Safety and Digital Security Law of The United Arab Emirates.

***Reference:*** https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

**DEFINITIONS:**

- **Cyber safety:** the way in which users behave responsibly online to keep themselves and their friends safe. It incorporates the safe and desirable use of the Internet and ICT equipment and devices, an awareness of our digital footprint, and how to behave appropriately and respectfully.
- **Online Threats to Students:** As well as the threats that all users face when going online, such as computer viruses and email scams, students are at risk from the following:
    - **Cyber bullying:** Cyber bullying is bullying that takes place over digital devices such as cell phones, computers, and tablets. Cyber bullying can occur through SMS, text, and mobile applications (apps) or online in social media, forums, or gaming where people can view, participate in, or share content. Cyber bullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else, causing embarrassment or humiliation. Some cyber bullying crosses the line into unlawful or criminal behavior.
    - **Inappropriate Content:** Adolescents and children can unintentionally come into contact with inappropriate content, such as sexually explicit material. Unsolicited obscene materials can also be received electronically.
    - **Sexting:** Sexting is the sharing and receiving of sexually explicit messages and nude or partially nude images via text messages or apps. Sexting, while commonly occurring off school grounds, also occurs on school property, with content being sent and viewed on cell phones. Of note is that possession of sexually explicit photos received by sexting can be considered a type of possession of child pornography from a legal perspective.
    - **Sextortion/Ransomware:** Students may also become victim to sextortion, possibly via ransomware, if they engage in sexting. Sextortion occurs when someone threatens to distribute private and sensitive material if not provided with images of a sexual nature, sexual favors, or money. Ransomware is a particular form of computer malware in which perpetrators encrypt users' files, and then demand the payment of a ransom for users to regain access to their data. Ransomware can also include an element of extortion, in which the perpetrator threatens to publish data or (possibly sexually explicit) images if the victim does not do what the perpetrator wants, such as provide nude photos.
    - **Oversharing:** Personal information that is sometimes shared by students includes their name, age, address, phone number, and Social Security number.
    - **Online Predation:** Online predators put victims through "the grooming process," a series of steps by which they build the victim's trust by sympathizing with him or her or feigning common interests, after which they proceed to set up a face-to-face meeting with the victim and then move forward with manipulation and seduction
    - **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 same interests as of the child.

## ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and groups within the New Indian School.

**GOVERNORS:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. One of the Governors will execute:

- Regular meetings with the Link Governor/E-Safety Coordinator.
- Regular monitoring of e-safety incident logs, maintained by the E-Safety Coordinator.
- Recommending necessary guidelines to ensure the effectiveness of the policy, at least twice a year.

**PRINCIPAL and SENIOR LEADERSHIP TEAM (THE DESIGNATED SAFEGUARDING LEADS)**

- The Designated Safeguarding Leads (DSL) are Senior Leadership Team Members 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 & Child Protection Policy.
- The DSL has overall responsibility for safeguarding arrangements within the School, including the NIS's approach to online safety and the use of technology within the School.
- The DSL are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Principal and The Link Governor 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.
- The Principal 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.

**THE LINK GOVERNOR (A Member from Senior Leadership Team)**

- The Link Governor assumes with the leadership responsibility for the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Governors.
- The LG will work with the E-Safety Coordinator 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.
- The LG will regularly monitor the Technology Incident Log maintained by the E-Safety Coordinator.
- The LG will regularly update other members of the DSL on the operation of the School's safeguarding arrangements, including online safety practices.

**E-SAFETY COORDINATOR:**

- Leads the e-safety Cluster Leaders
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the NIS e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the relevant body
- Liaises with NIS technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets/updates regularly with the Link Governor and discusses current issues, reviews incident logs and filtering / changes control logs
- Attends relevant meeting / committee of Governors and the DSL
- The E-Safety Coordinator has to ensure:
    - That the NIS's technical infrastructure is secure and is not open to misuse or malicious attack.
    - That the NIS meets required e-safety technical requirements, recommended by the relevant body of Government.
    - That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
    - That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
    - That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Link Governor.
    - That the NIS has an effective filtering policy in place and that it is applied and updated on a regular basis.
    - That the risks of students and staff circumventing the safeguards put in place by the NIS are minimized;
    - That the monitoring software and systems are kept up to date in order to monitor the use of email and the internet over the NIS's network and maintain logs of such usage.
    - That the NIS maintains 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.
- Provides 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.
- He 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 NIS's Child Protection & Safeguarding Policy and Procedures.

**THE CLUSTR LEADERS:**

They are the team facilitators and advocates of the E-Safety Policy and they promote the well-being of the students and staff through various programs.

- Initiates relevant events to instill the seriousness of Policy elements.
- Schedules frequent sessions with the respective cluster groups.
- Acts the roles of educators to all the stakeholders, esp. Students and Staff.
- Updates the Teaching staff with decisions and reviews of the E-Safety Meetings.

**E-SAFETY CURRICULUM COORDINATOR**

- Integrates relevant areas of Digital Citizenship into the general Curriculum across all the levels.
- Ensure the inclusion of major elements from Acceptable Use Policy and Unacceptable Use Policy.
- Liaises with I.T. Teachers to ensure the imparting of the relevant areas of E-Safety Policy.
- Ensure that students are evaluated terminally with the contents of E-Safety areas.

**TEACHING STAFF**

They are responsible for ensuring:

- That they are an up to date awareness of e-safety matters and of the current school / academy e-safety policy and practices
- That they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- That they report any suspected misuse or problem to any of the Cluster Leaders.
- That all digital communications with students / parents should be on a professional level and only carried out using official school systems
- That E-safety issues are embedded in all aspects of the curriculum and other activities
- That Students understand and follow the e-safety and acceptable use policies
- That Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- That they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- That in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**SUPPORTING STAFF**

- The NIS staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the NIS's policies and of safe practice with the students.
- Staff are expected to adhere, so far as applicable, to each of the policies.
- 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.

**CHILD PROTECTION LEAD:**

- Should be a trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - Sharing of personal data

- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

**STUDENTS:**

- Are responsible for using the NIS digital technology systems in accordance with the Student Acceptable Use 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 cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

**PARENTS:**

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 to any of the School Staff
- 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.

The school will take every opportunity to help parents understand these issues through various sessions, campaigns, mails, circulars and through website. Parents will be encouraged to support the School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the online classrooms and messenger portals
- Their children's personal devices in the School.

## POLICY STATEMENTS

**EDUCATION – STUDENTS**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognize and avoid e-safety risks and build their resilience.

**E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:**

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

**EDUCATION – PARENTS**

Many parents have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and caregivers through:

- Curriculum activities
- Mails, Circulars, website, etc.

- Parent Sessions
- Surveys and Competitions
- Reference to the relevant web sites / publications

**EDUCATION – THE WIDER COMMUNITY**

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- The school website will provide e-safety information for the wider community.
- Student Videos in social media to highlight the E-Safety measures.
- Supporting community groups (e.g. Youth / sports / voluntary groups) to enhance their e-safety provision

**EDUCATION & TRAINING – STAFF / VOLUNTEERS**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events or by reviewing guidance documents released by relevant organisations
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

**TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING**

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- The Principal / LG is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users

- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, Guest lecturers) onto the school systems
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

**Bring Your Own Device (BYOD)**

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

**USE OF DIGITAL AND VIDEO IMAGES**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for

employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognize the risks attached to publishing their own images on the internet, e.g. on social networking sites
- In accordance with guidance from the School Management, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents comment on any activities involving other students / pupils in the digital / video images
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents will be obtained before photographs of students are published on the school website
- Students' work can only be published with the permission of the pupil and parents.

**DATA PROTECTION**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

**THE SCHOOL MUST ENSURE THAT:**

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office

**STAFF MUST ENSURE THAT THEY:**

- At all times take care to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

**COMMUNICATIONS**

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students or parents' (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate

communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

**SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY**

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or The Ministry liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

**SCHOOL STAFF SHOULD ENSURE THAT:**

- No reference should be made in social media to pupils, parents / caregivers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or The Ministry.
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information

The School's use of social media for professional purposes will be checked regularly by the Safety Officer and e-safety committee will ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

## SCHOOL'S STRATEGY

The school employs a number of strategies in order to maximize learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

**GENERAL**

- Internet sessions will always be supervised by a teacher
- Filtering software and/or equivalent systems will be used in order to minimize the risk of exposure to inappropriate material
- The school will regularly monitor students' internet usage
- Students and teachers will be provided with training in the area of Internet safety
- Uploading and downloading of non-approved software will not be permitted
- Virus protection software will be used and updated on a regular basis
- The use of personal memory sticks, CD-ROMs, or other digital storage media in school, requires a teacher's permission
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute

**WORLD WIDE WEB**

- Students will report accidental accessing of inappropriate materials in accordance with school procedures
- Students will use the Internet for educational purposes only
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons

**EMAIL**

- Students will use approved class email accounts under supervision by or permission from a teacher
- Students will note that sending and receiving email attachments is subject to permission from their teacher

**COMMUNICATIONS**

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following shows how the school currently considers using these technologies for education:

- All are allowed to use hand held devices like PDAs, PSPs
- Official Communications on behalf of the School should be with the personal ID given by the School.
- Instant Messaging is commonly allowed.
- Blogs, designed for educational purposes are allowed to use.

**SCHOOL WEBSITE**

- Students will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of students or staff
- Website using facilities such as comments and user-generated content will be checked frequently to ensure that they do not contain personal details
- The publication of student work will be coordinated by a teacher
- The school will endeavor to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will only be published on the school website with parental permission
- Personal student information including home address and contact details will be omitted from school web pages
- The school website will avoid publishing the first name and last name of individuals in a photograph
- The school will ensure that the image files are appropriately named and will not use students' names in image file names or ALT tags if published on the web
- Students will continue to own the copyright on any work published

**PERSONAL DEVICES**

Students using their own technology in school should follow the rules set out in this agreement. They will only use personal hand held / external devices (Laptops/Tablets/ USB devices etc) in school if they have permission.

**SUPPORT STRUCTURES**

The school will inform students and parents of key support structures and organizations that deal with illegal material or harmful use of the Internet.

**SANCTIONS**

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

## ACCEPTABLE USE POLICY

We in the New Indian School are pleased to be able to offer our students, staff and guests access to computer technology, including access to the Internet, certain online services, and the School information technology network. We are dedicated to access and support of appropriate technology which unlocks our potential and connects us locally and globally. We envision a learning environment where technology is a part of us, not apart from us.

The aim of this Acceptable Use Policy (AUP) is to ensure that students will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

It is envisaged that school and parent representatives will revise the AUP annually.

Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

We believe that the tremendous value of technology and the information technology network as an educational resource far outweighs the potential risks. We will leverage existing and emerging technology as a means to learn and thrive in the 21st Century and prepare our students for success toward their goals in the competitive global, electronic age. We feel that access to the tools and resources of a world-wide network and understanding when and how these tools are appropriately and effectively used are imperative in each student's education. However, if parents feel they do not want their child to have Internet access, then they will be responsible for informing their child's teachers, in writing, before the end of the second week of school.

The school's information technology resources, including email and Internet access, are provided for educational purposes. If you have any doubt about whether a contemplated activity is acceptable, consult with your immediate teacher, supervisor, or director to help decide if a use is appropriate. Adherence to the following policy is necessary for continued access to the school's technological resources:

**Users must respect and protect the privacy of others by:**

1. Using only assigned accounts.
2. Only viewing, using, or copying passwords, data, or networks to which they are authorized.

3. Refraining from distributing private information about others or themselves.

**Users must respect and protect the integrity, availability, and security of all electronic resources by:**

1. Observing all school Internet filters and posted network security practices.
2. Reporting security risks or violations to a teacher or network administrator.
3. Not destroying or damaging data, networks, or other resources that do not belong to them, without clear permission of the owner.
4. Conserving, protecting, and sharing these resources with other users.
5. Notifying a staff member or administrator of computer or network malfunctions.

**Users must respect and protect the intellectual property of others by:**

1. Following copyright laws (not making illegal copies of music, games, or movies).
2. Citing sources when using others' work (not plagiarizing).

**Users must respect and practice the principles of community by:**

1. Communicating only in ways that are kind and respectful.
2. Reporting threatening or discomforting materials to a teacher or administrator.
3. Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct or honor code (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).
4. Not intentionally accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
5. Not using the resources to further other acts that are criminal or violate the school's code of conduct or honor code.
6. Avoiding spam, chain letters, or other mass unsolicited mailings.
7. Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

**Users may, if in accord with the policy above:**

1. Design and post web pages and other material from school resources.
2. Communicate electronically via tools such as email, chat, text, or videoconferencing.
3. Install or download software, if also in conformity with laws and licenses.
4. Use the resources for any educational purpose during school hours.

**Consequences for Violation**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. The school is responsible for sourcing and implementing relevant and developmentally appropriate programs and strategies that promote positive online behaviors and cyber safe practices. Violations of these rules may result in disciplinary action, including the loss of a user's privileges to use the school's information technology resources. Further discipline may be imposed in accordance with the school's code of conduct and honor code up to and including suspension or expulsion depending on the degree and severity of the violation.

**Supervision and Monitoring**

The use of school owned information technology resources is secure, but not private. School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy.

Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.
The school reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The school also reserves the right to limit the time of access and use.

## GENERAL GUIDELINES

**RESPONDING TO INCIDENTS OF MISUSE**

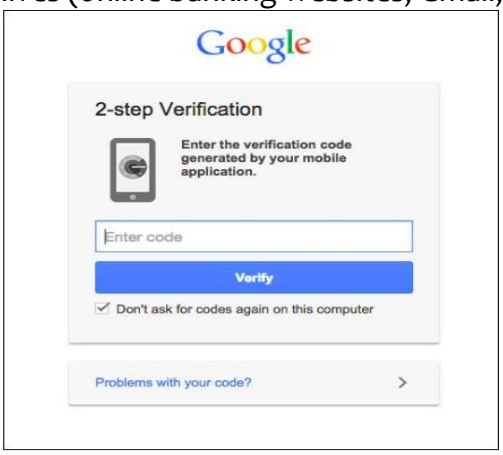
- This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

**ILLEGAL INCIDENTS**

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

**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. E
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.

**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 internet for 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.

**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?**

- Share with your parents or elders in family
- You can ask your parents to write a mail to the school counselor at safety@nisuaq.com /counsellor@nisuaq.com
- Ask your parents to contact the section supervisor of your respective section. The numbers are given as below.
    1. Ms. Amatour Sara (KG Section) : 0504977264
    2. Ms. Amtul Basheer (Primary Section) : 0567265775
    3. Ms. Laisa Kuttan (High School Section) : 0503074489

**TECHNICAL ASPECT**

Use safe search options while searching information on the Internet; also check facts before sharing or forwarding.

- While performing online banking, shopping or making online payment, check if the website's URL begins with 'https' (the "s" stands for "secure"), also, look for a green address bar or a security certificate (presented by an icon such as an unopened lock) in the browser window that ensures secure connection. Double click the certificate to make sure the name on the web address matches the certificate.
- Use a strong and unique password combinations of numbers, uppercase, lowercase letters and special characters for each account.
- Use separate email accounts for personal and official purpose.
- Delete old accounts that you do not use any more.
- Obtain software from trusted sources. Always scan files before opening them.
- Access your bank's website by manually typing its URL in the address bar. Never access it from an email or a text message.

- Never click on links or download attachments in unwanted, unexpected emails, even if such emails appear like they are from a known source.
- Take regular backups of all important files onto offline/ cloud storage.
- Don't click on ‘Keep me logged in’ or ‘Remember me’ options on websites and logout of all accounts..
- Never use any personal information such as name, date ofbirth, address, etc., as your password.
- Never share your personal/bank details on phone, email or SMS, even if the caller/sender seems genuine.
- Think before you click; stay away from pop-up contests and shady surveys; read the fine print, and close all such pop-ups from the task manager
- Don't visit inappropriate websites, or websites that you are not fully aware of, just out of sheer curiosity.
- Don’t save your credit/debit card information on websites and web browsers.
- Connect to proper wi-fi network, otherwise known as SSID.
- Have dual or multifactor authentication.
- Don't use username and password when other options as such as a token, smartcard, PIN, or even user-selected security images are available.
- Maintain a list of passwords in a safe place, and change them at least quarterly.
- Ensure that the computer has the latest patches and keep the browser, operating system and antivirus updated.
- Don't assume that the virus detection software works perpetually with computers.
- Don’t share/ upload confidential data in cloud storage systems .
- Keep a record of all online transactions made and check your bank account regularly.
- Add a Domain Name System (DNS) service to protect other devices.
- Lock your screen when you have finished using your computer/ tablet/ phone, and further, set it to lock automatically when it goes to sleep.
- Don't assume someone else has the responsibility to maintain and protect your data.
- Do check e-mails carefully to ensure that the source header is from a valid address.
- Don't fall prey to clicking a link to malicious Web sites that load malware into your computer.
- Always delete spam emails immediately and empty the trash box to prevent accidental clicking on the same link While interacting with others on discussion forums/ chat rooms, make sure the Caps Lock key is off as typing in capital letters during interaction is considered to be rude.
- Monitor device usage by students; control time spent on devices.
- Create restricted or child-only profiles - use options available on browsers, Search, video sites, etc.
- Ensure that students access only the content/ sites allowed to them
- Regularly review browsing history on the devices being used by children.

**ETHICAL ASPECTS**

- Don’t intentionally use the computers to retrieve or modify the information of others, which may include password information, files, etc.

- Don’t plagiarize i.e., copying information (book, music, video, software etc) from the Internet as it is dishonest and could also be illegal. You could be violating copyright laws.
- Obtain permission from the original creator if you do want to use the material.
- Always provide credit and attribution to the original owner of the resource.
- Never give a fake identity while interacting with people online.
- Do not make profit from the original work of others Use of material upto 10% may be done by citing the resource. Paraphrase wherever possible.

**SOCIAL ASPECTS**

- Avoid sharing your personal information on social media sites and the Internet in general.
- Don't cyber bully by being rude,or by using abusive, threatening, humiliating language.
- Don't engage or argue with cyberbullies as that might encourage even worse behavior.
- Use the built-in filters to prevent further harassment through email or instant messaging by cyber bullies.
- Never meet people alone when they are known only through online.
- Don’t do anything online which cannot be done in the presence of others.
- Monitor students’ behavioral changes or attitude differences.

**LEGAL ASPECTS**

- Do report cyber bullying to the proper authorities. Keep a record of every comment received from a cyberbully for taking further action.
- Never trust e-mails which offer prize money through lotteries of which you are not a participant. Similarly don't pay for the jobs which you have not sought through official channels.
- Don't trust a site just because it claims to be secure. It may be a 'Phishing' site.
- Beware of e-mail spoofing.
- Beware of fake advertisements promoting online purchases.
- Don’t buy any device from unauthorized persons/ dealers.
- Never read someone else's e-mails even if you know his/her password.
- Never tamper with the computer source records.
- Never share or alter the collected data without permission of the individual/ organisation.
- Never capture, reproduce or transmit the photograph(s) of a person without his/ her consent.
- Never publish or transmit vulgar material in electronic form.
- Report any objectionable child-abusive materials in electronic form to the concerned authorities.
- Don't send any threatening, abusive or defamatory emails.
- Don’t hide/ conceal computer hardware belonging to school.
- Never infringe on any copyrighted materials.

## GUIDELINES FOR STUDENTS

- **DOs**

  1. Respect the privacy of others.
  2. Report and flag content that is abusive or illegal.
  3. Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.

4. Use an alias/ alternate name as username when you interact/ chat with others online.
5. Report online bullying immediately to the teacher and parents/ or some one whom you trust.
6. Use a strong and unique password with combinations of numbers, uppercase and lowercase letter and special characters for each account(s).
7. Keep the browser, operating system and antivirus up-to-date.
8. Obtain software from trusted sources. Always scan files before opening them.
9. Lock your screen when you're finished using your computer/ tablet/ phone. Further, set it to lock automatically when it goes to sleep.
10. Check to see if the web address begins with https:// whenever you sign in online.
11. Make privacy settings in social media accounts in such a way that profile and posts are visible only to close friends and acquaintances.
12. Connect only with known individuals.
13. Be mindful of your digital reputation - think twice before you post something embarrassing, harmful or inappropriate.
14. Report to the service provider immediately if the account is hacked. If possible deactivate your account.

**DONTS**

1. Don't share your personal information: real name, date of birth, phone number etc. unnecessarily.
2. Don't send your pictures to unknown persons or share them on social media.
3. Don't open emails and attachments from strangers.
4. Don't respond to any suspicious email, instant message or web page asking for personal information.
5. Don't enter a password when someone is sitting beside you as they may see it.
6. Don't share your password with anyone.
7. Don't save your username and password on the browser.
8. Don't steal other's information.
9. Don't access or use files without the permission of the owner.
10. Don't copy software which has copyright without the author's permission.
11. Don't bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.
12. Don't use someone else's password even if it is shared with you.
13. Don't log in as someone else to read their emails or mess with their online profiles.
14. Don't attempt to infect or in any way try to make someone else's computer unusable.
15. Don't meet unknown (even if they are known only through online interaction) people alone; always inform an adult or a friend.
16. Don't open or download any attachments from an unknown source as they may contain viruses.

**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.

## CONCLUSION & EVALUATION

Due to the rapid evolution of ICT, regular evaluation and updating of this policy will occur as and when required by the school leadership. ICT team will constantly monitor the tidings in vogue and will foresee the futuristic developments regularly and constantly and make amends in the said policy as and when required.

The school will monitor the impact of the policy using: (delete / add as relevant)

- Logs of reported incidents
- Surveys of reported incidents.