Cyber Safety and Security Policy

2023-2024

المدرسة الهندية العالمية الخاصة
INTERNATIONAL INDIAN SCHOOL

Creation date: September 2018
Last amendment date: April 2023
Next review date: April 2024
Prepared by School Council Members

Members of the committee

- Mr. Wasim Yousuf Bhat (Dean)
- Mr. Qurat al Ain (Principal)
- Mr. Mujeeb Rahman (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	Term Wise
Review of the policy	Term wise
Next anticipated Review date	April 2024

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, staffs 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.

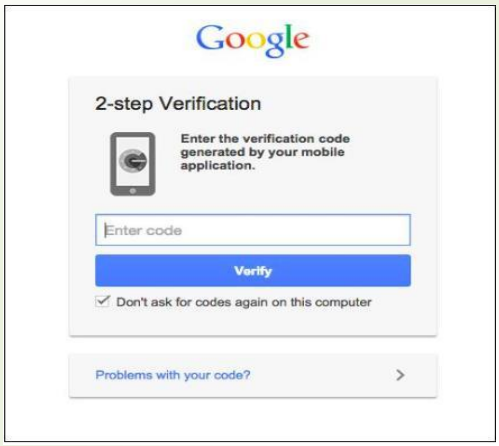
The DONT's in the use of Technology and Electronic Communication:

- 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.
- Donʻt 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 otherʻs information.
- Donʻt access or use files without the permission of the owner.
- Don't copy software which has copyright without the authorʻs 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 same interests as of 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 incase 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 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.

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. Mary Samna I S, the social worker

Email id: osl@iisajman.org

Contact No: 0505742741

Other Contacts

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

Contact No0503867361

Name: Ms. Jagrita Mazumdar , Primary 1 section Head, Email id primary1@iisajman.org Contact No: 0547440169

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

Contact No:0507460864

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

Contact No: 0567424054

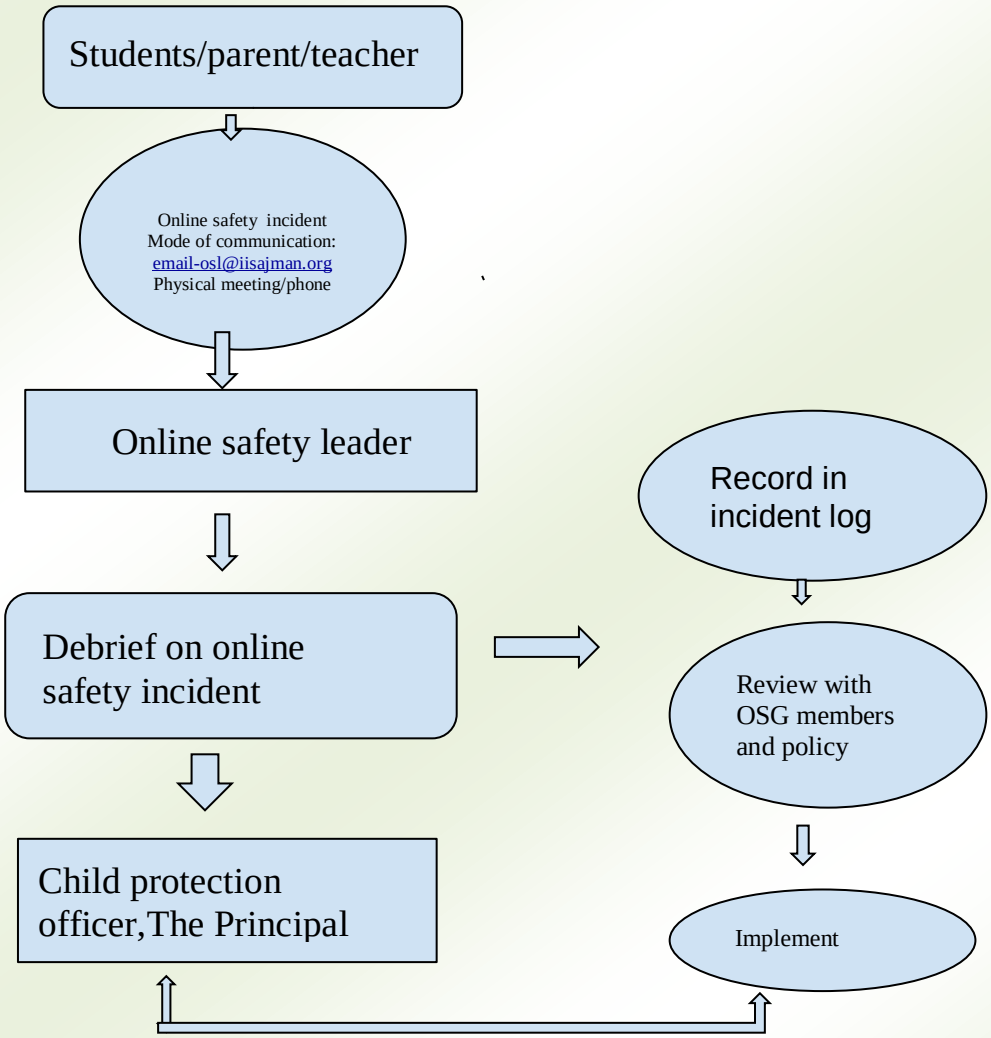
Mr. Jayakrishnan Boys section section head, Email Id: boyssection@iisajman.org

Contact No: 0505313380

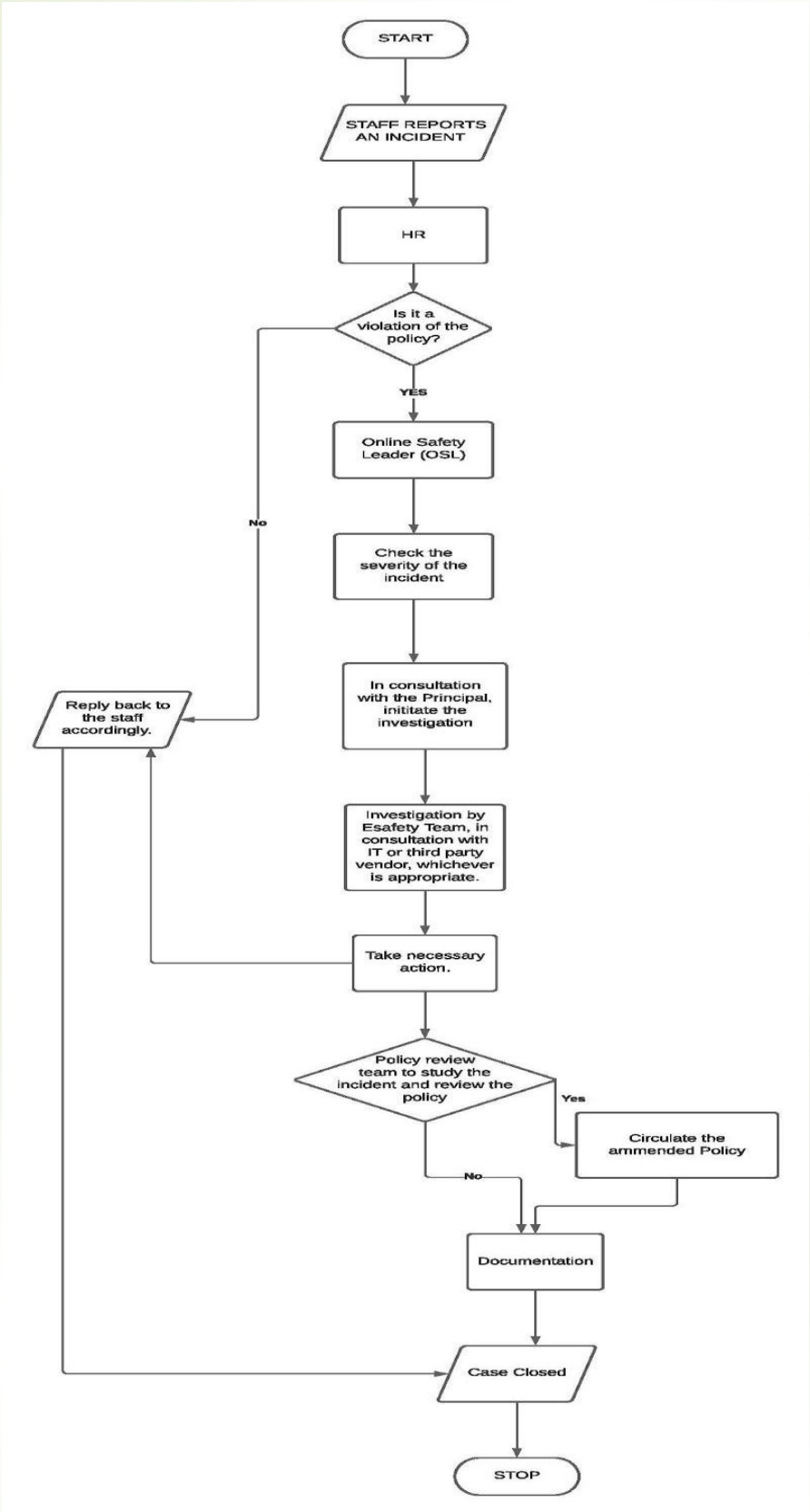
Ms. Qurat Ul Ain , the principal , Child protection officer, Email Id: principal@iisajman.org

Contact No: 0558403796

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

Online Safety Group and Responsibilities

Governor	Mr. Wasim Yousuf , Dean AI
Child protection officer	Ms. Qurat Ul Ain, Principal
Online safety Leader	Ms. Mary Samna I S, Social Worker
Senior Leader (Section heads)	Ms. Jagrita, Ms. Rekha, Ms. Hilda & Mr. Jayakrishnan
Tech Support	Ms. Reshma A, Software Analyst Mr. Sabeel K, System Admin
Teachers' Representative	Ms.Fathima Banu, KG Ms. Sandya, primary 1 Ms. Hajout Kaur, primary 2 Ms. Rajeswary Alakkal, girls section Ms. Irfana, boys section
Parents' Representative	Mr. Sajeer Mon CK, P/O Faliha CK KG IMs. Faarah Azmat, P/O Mahnoor 2L Ms Sumayya Mohammed, P/O Shayna 6G Ms. Diju, P/O Bilal 4D Mr. Hamza Shahaban,P/O Misbah 9D
Student' Representative	Aadidev .K Grade 2B, Gr No11211 Nearysa Patel 2H, Gr No 11338 Sahil Rasheed 4G,Gr No 9457 Riddhi Sivadasan, 4H, GR No 9452 Angelina Edward 11G Gr NO 9959 Abijith Aji, 12A-Gr No-6632
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.

CPO- 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 E-Safety 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.

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 falls 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 to 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 cyber-bullying.

• 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 program 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 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 staffs require training through 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 (eg 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

PASSWORD POLICY

Introduction

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform). You can find out more about passwords, why they are important and how to manage them in our blog article. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important.

Effective password management will protect International Indian School's data and reduce the risk of unauthorized applications access. The policy is to establish a secure information technology environment by enforcing the use of strong passwords. Strong and complex password are the front line of protection for user's accounts. A poorly chosen password may result in the compromise of International Indian School's entire network. The purpose of this policy is to provide standards for defining domain passwords to access International Indian School IT resources such as email, academic and administrative applications, computing labs and School-owned computer systems for protecting International Indian School data and reducing the risk of unauthorized access by enforcing the use of strong passwords.

Scope

This policy shall apply to all employees, students, and parents of International Indian School School, and shall govern acceptable password use on all systems that connect to International Indian School School network or access or store International Indian School School's data.

Policy

- These statements apply to all stakeholders (Staff, Students, Parents, Vendors) of International Indian School.
- All school networks and systems will be protected by secure passwords.
- All users are clearly defined with the access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Administrator and will be reviewed, at least annually, by the online safety group.
- All stakeholders have responsibility in securely keeping the login credentials. Ensure that other users are not accessing the systems using other user's login credentials. Any breach of security or suspicious incidents must be immediately reported with evidence.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by IT Administrator who will keep an up to date record of users and their usernames

Password

- Passwords should be long and must be over 8 characters in length.. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password must contain uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts. This will ensure that other systems are not put at risk even if anyone account is compromised.
- Passwords must not contain any personal information about the user that might be known by others
- Passwords must be changed on the first login to the system itself.
- Passwords must not kept in writing or electronically which can be accessible by others.

- Records of learner usernames and passwords for younger students/pupils are securely kept which is accessible only by the IT administrator.
- Password complexity for younger students is less (5-character maximum) and special characters are not included.
- Password requirements for older students are more complex (8 characters minimum) including special characters.
- Users are required to change their password if it is compromised. The school will reset passwords at the start of each academic year to avoid large numbers of forgotten password reset requests where there is no user-controlled reset process.
- Student will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.
- Password enforcing will be applied to all users and systems in regular intervals (3 months) and whenever a compromise threat is detected by the IT administrator.
- The administrator have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration is given using two factor authentication for such accounts.
- An administrator account password for the school systems is kept in a secure school safe. This account and password is only used to recover or revoke access. Other administrator accounts does not have the ability to delete this account.
- Any digitally stored administrator passwords is hashed using a suitable algorithm for storing passwords
- There is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Wherever user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users is allocated by

administrator. This password should be temporary and the user should be forced to change their password on first login.

- Where automatically generated passwords are not possible, administrator will provide the user with their initial password. There is a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password is temporary and the user will be forced to change their password on the first login.

- Requests for password changes is authenticated by administrator to ensure that the new password can only be passed to the genuine user

- Suitable arrangements are provided to visitors with for appropriate access to systems which expires after use. The technical team will provide pre-created user/password combinations that will be allocated to visitors, recorded in a log, and deleted from the system after use.

- All the user accounts will be "locked out" following six successive incorrect log-on attempts.

- Passwords will not be displayed on screen, and will be securely hashed when stored.

Training/awareness

It is essential that users are made aware of the need for keeping passwords secure, and the risks attached to unauthorized access/data loss. This apply even to the youngest of users. All stakeholders are taught how passwords are compromised, so they understand why things should be done a certain way

Members of staff will be made aware of the school's password policy

- During induction
- school 's online safety policy and password security policy
- acceptable use agreement

Students/pupils will be made aware of the school's password policy

- in lessons
- through the Acceptable Use Agreement
- Through activities

Audit/monitoring/reporting/review

- The IT Administrator will ensure that full records are kept of:
- User Ids and requests for password changes
- User logons
- Security incidents related to this policy

Unacceptable Use

- Any breach of password policy will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate as per the reporting mechanism.
- Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take necessary action.

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

This policy is linked with all the other policies of the School.

FILTERING POLICY

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Scope

This policy applies to all anyone accessing the Internet on devices that are connected to the IIS AJMAN network, including School owned, personally owned, and mobile devices.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by IT ADMINISTRATOR. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs
- be reported to IT administrator
- *be reported to and authorized by IT administrator prior to changes being made*
- *be reported to the Online Safety Group every 6 months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to IT ADMINISTRATOR any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *The school maintains and supports the managed filtering service provided by the Internet Service Provider* – As per UAE TRA (Telecommunications Regulatory Authority)
- *The school manages its own filtering service*
- *The school has provided enhanced/differentiated user-level filtering through the use of the filtering programme. (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal (or other nominated senior leader).*
- *Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*

Requests from staff for sites to be removed from the filtered list will be considered by the IT ADMINISTRATOR . The *IT ADMINISTRATOR*, in conjunction with the online safety group, will periodically review and recommend changes to Internet filtering rules. Senior Leadership shall review these recommendations and decide if any changes are to be made.

Education/Training/Awareness

Pupils/students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- Induction training
- Staff meetings, briefings.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions/newsletter etc.

Changes to the Filtering System

If a website is blocked, employees should consult with their manager before requesting an exception. Managers may submit a request to review a blocked website by contacting the International Indian IT Administrator. The Network Admin will review the request, will communicate updates to the employee and Manager, and will consult with vendors, as well as the School Online Safety team, as needed.

- if the Network LAN Admins determine a website is properly categorized per our security systems, the security team shall be consulted to decide if changes are to be made, such as unblocking the website, if proper business justification has been documented by the employee and manager.

- if the site is confirmed to be mis-categorized, the Network LAN Admins may unblock the site until the necessary changes are released by the vendors.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to IT ADMINISTRATOR who will decide whether to make school level changes.

- All categories other than below mentioned are blocked in School network.
- Arts and culture
- Education
- Health and wellness
- News and media
- Sports
- Information and computer security
- Information technology
- Online meeting

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated

in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:*

Audit/Reporting

- Logs of filtering change controls and of filtering incidents will be made available to:
- IT Administrator
- Online Safety Group
- External Filtering provider

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

School IT dept. provides an effective filtering system, as a result of which the following categories of websites are not, by default, available to schools: -

- ***Adult:*** content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity;
- ***Violence:*** content containing graphically violent images, video or text;
- ***Hate Material:*** content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds;
- ***Illegal drug taking and the promotion of illegal drug use:*** content relating to the use or promotion of illegal drugs or misuse of prescription drugs;
- ***Criminal skill/activity:*** content relating to the promotion of criminal and other activities;
- ***Gambling:*** content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

Access to network:

Access to the network is provided through password authentication using WPA. This key is not available to any staff aside from the school. Access is therefore governed by unique device registration and pre approval.

Hardware and general service provision:

The following has been installed and configured in school to ensure only appropriate content is available to all users:

1. A hardware firewall filter is installed which intercepts all Internet traffic leaving and entering the school network and this cannot be circumvented. This firewall appliance is configured for the Global view Internet filtering service. This service is a professional, commercial category based web filtering solution in use. It uses a category based system to group web sites in addition to keyword, Content filtering, IP and specific white and blacklist control. School licenses are purchased on a fixed three year term to ensure continuity of service and the individual firewall is monitored 24/7 with instant notification of any concerns.

2. In addition, IP and URL black and white listing is supported locally which ensures any content that is flagged as non-desirable on the network, can be disabled immediately.

3. Full access logs are maintained for all traffic and all attempts at access of inappropriate content.

Enforcement

The Network Admins and the School Online safety team will periodically review Internet use filtering systems and processes to ensure they are in compliance with this policy.

MOBILE DEVICE POLICY

Purpose & Scope:

The purpose of this policy is to define standards for end users who have legitimate business requirements to use a private or School provided mobile device that can access the School's electronic resources. This policy applies to, but is not limited to, the use of mobile/cellular phones, laptop/notebook/tablet computers, smart phones and PDAs, and any mobile device capable of storing corporate data and connecting to an unmanaged network, hereinafter referred to as "mobile device."

The goal of this policy is to protect the integrity and confidential data that resides within International Indian School's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised.

A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to International Indian School's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of International Indian School's direct control to backup, store, and otherwise access International Indian School data of any type must adhere to International Indian School - defined processes for doing so.

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational and that this is irrespective of whether the device is school owned/provided or personally owned.. The mobile technologies policy is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

Policy

- The school allows:

	School / Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised Device	Pupil / Student owned	Staff owned	Visitor owned
Allowed in school	No	Yes	Yes	No	Yes	Yes
Full network access	No	No	No	No	No	No
Internet only	Yes	Yes	Yes	No	Yes	Yes
No network acces				Yes		

- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete/amend as appropriate):
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
- *All school devices are subject to routine monitoring*
- *Pro-active monitoring has been implemented to monitor activity*
- *When personal devices are permitted:*
- *All personal devices are restricted through the implementation of technical solutions that*

provide appropriate levels of network access

- *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
- *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
- *The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues*
- *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
- *The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
- Personal Devices may not be used in tests or exams
- Visitors are provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site and on school buses
- School devices are provided to support learning. It is expected that pupils/students will bring devices to the school as required.
- Confiscation and searching - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness,

etc…) that would stop the device working as it was originally set up and intended to work is not permitted

- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps

- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students/pupils on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.

- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.

- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately

- *Devices may be used in lessons in accordance with teacher direction*

- *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*

- *Printing from personal devices will not be possible.*

Employees are expected to use good judgment when engaging in personal calls, sending/receiving text messages, and/or Internet usage on their mobile device during work hours. Excessive personal calls, text messaging, and/or Internet usage during work hours regardless of the phone used can interfere with employee productivity, safety and be distracting to others. Employees who make excessive or inappropriate use of a mobile device may be limited to using such devices only on scheduled break periods.

To protect the privacy of the faculty, staff, students and visitors, employees are prohibited from using their mobile device as a means to photograph and/or record an individual(s) in any form (audio and/or video) without that individual's knowledge and consent.

The use of mobile devices to photograph and/or record confidential information, private information and/or related item is prohibited. International Indian School will not be liable for the loss of personal mobile devices brought into the workplace. Any connection to the School's information services must adhere to the Acceptable Use of Technology Policy.

Employees may not use any cloud-based apps or backup that allows company- related data to be

transferred to unsecure parties. Certain employees may be issued a school owned mobile device. Use of these devices is contingent upon continued employment with International Indian School and the device remains the sole property of International Indian School. Excessive use of minutes or bandwidth for non-business activity is discouraged and may result in a Payroll deduction for personal usage.

Upon resignation or termination of employment, the employee may be asked to produce the mobile device and it will be reset to factory defaults using the remote wipe software. International Indian School will not be responsible for loss or damage of personal applications or data resulting from the remote wipe.

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

This policy is linked with all the other policies of the School.

DATA PROTECTION POLICY

SCHOOL PERSONAL DATA HANDLING

Recent publicity about data breaches suffered by organizations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organizations. It is important that the school has a clear and well understood personal data handling policy in order to minimize the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorized or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organizational reputation
- schools/colleges are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school will want to avoid the criticism and negative publicity that could be generated by any personal data breach
- the school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation
- It is a legal requirement for all schools to have a Data Protection Policy and be able to demonstrate compliance with data protection law.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in the school but also from remote locations. It is important to stress that the data protection laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent local/external regulations and guidance and changes in legislation.

INTRODUCTION

International Indian School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

This policy is intended to ensure that personal information is dealt with correctly and securely. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines. It is the responsibility of all members of the school community to take care when handling, using or transferring personal data, that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the School head. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance

SCOPE & OBJECTIVE

This is a policy that applies to all Users and all Systems.

“Users” are everyone who has access to any of the school's IT systems. This includes permanent employees and also temporary employees, parents, students, contractors, agencies, consultants, suppliers, customers and business partners. “Systems” means all IT equipment that connects to the School network or access school applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

PERSONAL DATA

The school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is information

that relates to an identified or identifiable living individual This will include:

- personal information about members of the school community – including students/pupils, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- curricular / academic data e.g. class lists, student/pupil progress records, reports, references
- professional records e.g. employment history, taxation and insurance records, appraisal records and references any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

SECURE STORAGE OF AND ACCESS TO DATA

-

The school ensures that systems are set up so that the existence of protected files is hidden from unauthorized users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords made up from a combination of simpler words and must ensure all passwords comply with the school's safe password policy. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data (desktops and laptops) should be secured with a lock-on- idle policy active after at most 5 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

All paper based personal data must be held in lockable storage, whether on or off site. Users must

at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the school's systems by whatever means and must report any actual or suspected malware infection immediately.

BACKUP AND DISASTER RECOVERY POLICY

International Indian School critical servers are backed up automatically by Iperius on regular intervals. IT personnel regularly monitor and verify the backup process and files. In case of a server failure a new server can replace the existing one by restoring the Backup on the new server. Verification and monitoring process is in place and quarterly backups are restored and verified.

A centralized antivirus system is functional at International Indian School to tackle the viruses and Trojans. Gateway firewalls are also up and running in order to secure the internet and email communication. The firewall works to prevent the users from watching unintended materials, torrent downloading etc. As per the levels set by the administration some of the users have the rights over some areas of the internet for educational and research purposes.

SECURE TRANSFER OF DATA AND ACCESS OUT OF SCHOOL

The school recognizes that personal data may be accessed by users out of school or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorized premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorized user from outside the organization's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software

DISPOSAL OF DATA

The disposal of personal data, in either paper or electronic form,is conducted in a way that makes reconstruction highly unlikely. Electronic files are securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated. A Destruction Log is kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

DATA BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

The school have policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

TRAINING & AWARENESS

All staff should receive data handling awareness/data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / training sessions
- Day to day support and guidance from System Controllers

ENFORCEMENT

It is the responsibility of the end user to ensure enforcement with the policies above. All concerns, questions, suspected breaches, or known breaches shall be immediately reported to the Data Protection Officer.

REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 1 year. The policy review will be undertaken by the Principal, or nominated representative.

CONTACT

If you have any queries or concerns regarding this policy then please contact itsupport@iisajman.org

FAIR PROCESSING NOTICE

What is the purpose of this Notice?

The school is committed to respecting your privacy and protecting your personal information.

This Notice is intended to provide you with information about what information we are gathering about students, parents and staff, how and why we process this information.

What information do we collect?

The type's information that we collect include:

- Names, contact details including emergency contacts
- Characteristics such as language, nationality, country of birth.
- Medical information
- Admissions information
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Information relating to student behaviour
- Attainment records and assessment results
- Reported accidents
- Safeguarding information
- Special educational needs information
- Photographs
- CCTV footage

We may also receive some information from MOE and other schools.

How we collect information?

We may collect information from you whenever you contact us or have any involvement with us for example when you:

- Approach for admission enquiry / registration
- Create or update a profile in our website
- Take part in our events
- Contact us in any way including online, email, phone, SMS, social media or post where we collect information from

What is the purpose of collecting and using information?

The purposes for which the School collects personal information are as follows: -

- To manage admissions
- To complete registration process as per MOE requirements
- To support children with medical conditions, allergies and Special Education Need students (SEN) or students of determination.
- To monitor attendance
- For assessment and examination purposes
- For health and safety purposes
- To address safeguarding concerns
- To promote the school and celebrate educational achievement
- To ensure that the school is safe and secure
- To allow cashless payments to be made

Who will we share information with?

We do not share information about our students, staff and parents with anyone without consent unless the law and our policies allow us to do so.

We share information with:

- Legal entities like MOE, CBSE etc.
- Service providers who provide learning platforms and communication tools. We select our third party service providers with care. We provide these third parties with the information that is necessary to provide the service and we will have an agreement in place that requires them to operate with the same care over data protection as we do.

How we keep your information safe?

We understand the importance of keeping your personal data secure and take appropriate steps to safeguard it.

We always ensure only authorised persons have access to your information, which means only our employees and vendors, and that everyone who has access is appropriately trained to manage your information.

We reserve the right to amend this privacy statement in the future. Any changes we make to this notice will be posted on this page and where appropriate, notified to you by email.

POLICY FOR THE SAFE USE OF PHOTOGRAPH AND VIDEOS

Introduction

This policy covers the safe use of photographs and videos that covers staff and students. The use of photographs and videos plays an important role in school activities. Teachers or staff may use these photos or videos for presentations reports or on school display boards.

Photographs or videos may also be used to celebrate the success – for showcasing its academic and extracurricular standards on reports, printed or digital mediums and occasionally in the public media. The school will comply with the Data Protection Act and request parent's/carers permission before taking images or videos or students/staff. In case of sharing the images of student or staff on public media, only first name or initials will be shared, unless the parent feels it is relevant to include the complete name in case of any achievement.

Following guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their personal use. To respect everyone's privacy, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital/video images. Images of any third person, who is coming in such photographs should be blurred to respect their privacy. Teachers are not allowed to use and share the photos of any students on their profiles as posts, or status updates.

While taking photos/ videos of students, staff should ensure that the students are dressed as per the rules and standards of the school and are not participating in activities that might bring the individual or the school into disrepute. Photos or videos taken would not be manipulated or amended but can be cropped.

Aim of the Policy

- To enhance the school activities by adding a ray of colours through articles and photos.
- To help parents and the local community to identify and celebrate the schools' achievements.
- To increase pupil motivation and staff morale
- To promote a way of community spirit within the varsity
- To encourage parents and students to share their inputs and feedback
- To ensure the privacy and security of students, teachers and staff
- To ensure that all digital content published is keeping the guidelines of the policy

A photography consent form is shared with parent/carer/staff to take their permission before the use of image or video. Since the school collects personal information through this form the parents will be well informed about the below-mentioned information

Photography Consent Form

- School Principal, Academic Secretary, School Media Coordinator and Habitat School Group's Media Coordinator will have the access to this form.
- The form is stored at the office of the School Academic Secretary, along with the documents of the students/staff.
- Each form will be kept for two Academic Years and will be disposed of properly (Soft copies will be deleted and hard copy will be shredded) upon the completion of the year/once the student/staff leaves the school. However, the parent/carer/staff is free to change or update the permission at any point in time.

The use of images

- The photos/videos will be used on the platforms including the School website, School Social Media Pages including Facebook, Instagram, Twitter, YouTube, and LinkedIn. School official blog, Printed ads including Newspaper and Magazines, Outdoor ads including Flex, Lamppost ads, Mega coms.
- School Principal, Academic Secretary, School Media Coordinator and Habitat School Group's Media Coordinator will have the access to these photos/videos.
- Images/videos are saved digitally and shared with the concerned persons as google folders.
- Images/Videos will be stored for two Academic Years
- Images/Videos will be stored digitally and will be deleted upon the completion of two years
- In case the student/parent/staff wants to remove a photo that is uploaded online, a request can be forward to the school media coordinator to remove the file.

Re-use of Photos/Videos

No students, teachers or staff are allowed to download or copy the photos or videos published on the school official pages for their personal use with or without the parent's consent. Such usages will be a violation of the Data Protection legislation. However, they are allowed to share the post or videos as it is from the official pages.

Concerns

In case of complaints against the inappropriate usage of photographs or videos, a request can be forward to the school media coordinator through the student's class teacher.

COMPUTING & ICT POLICY

At school, we believe that Computing is an integral part of preparing children to live in a world where technology is continuously and rapidly evolving, so much so that children are being prepared to work with technology that doesn't even exist yet. For this reason, we feel that it is important that children are able to participate in the creation of these new tools to fully grasp the relevance of and the possibilities of emerging technologies thus preparing them for the world of work.

Purpose

The school follows the Cyber Square curriculum for Grade 1 to Grade 8. For Grade 9,10, 11 and 12 the school follows CBSE curriculum. High quality teaching of Computing, from Grade 1 to Grade 8, utilises a combination of practical lessons and theory lessons designed to promote discussion and nurture understanding, which are also relevant to other areas of the curriculum.

This policy reflects the values and philosophy in relation to the teaching and learning of and with computer science. This policy should be read in conjunction with the scheme of learning for Computing that sets out in detail what children in different year groups will be taught and how computer science can facilitate or enhance learning in other curriculum areas.

Aims

Computer Science

- To enable children to become confident coders on a range of devices.
- To create opportunities for collaborative and independent learning.
- To develop children's understanding of technology and how it is constantly evolving.

Digital Literacy

- To enable a safe computing environment through appropriate computing behaviours.
- To allow children to explore a range of digital devices.
- To promote pupils' spiritual, moral, social and cultural development.

Information Technology

- To develop ICT as a cross-curricular tool for learning and progression.
- To promote learning through the development of thinking skills.
- To enable children to understand and appreciate their place in the modern world.

Objectives

In order to develop the Computing and ICT capability and understanding of each child we will provide through our planning:

- Computing through all three strands taught within the classroom.
- Continuity throughout the school to ensure that experience and skills are developed in a cohesive and consistent way.
- Access to computers within class or in designated communal areas.
- Experience of a variety of well-planned, structured and progressive activities.
- Experience cross-curricular links to widen children's knowledge of the capability of computing including safe use of the Internet and other digital equipment.
- Opportunities for children to recognize the value of computing and ICT in their everyday lives and their future working life as active participants in a digital world.

Equal Opportunities, Inclusion, Special Educational Needs and Disabilities (SEND)

It is our policy to ensure that all children, regardless of race, class or gender, should have the opportunity to develop computing and computer science knowledge. We aim to respond to children needs and overcome potential barriers for individuals and groups of children by:

- Ensuring that all children follow the scheme of learning for Computing.
- Providing curriculum materials and programmes, which are in no way class, gender or racially prejudiced or biased.
- Providing opportunities for our children who do not have access at home to use the school computers/Internet to develop independent learning.
- Providing suitable challenges for more able children, as well as support for those who have emerging needs.
- Responding to the diversity of children's social, cultural and ethnographical backgrounds.
- Overcoming barriers to learning through the use of assessment and additional support.
- Communication or language difficulties by developing computing skills through the use of all their individual senses and strengths.

- Movement or physical difficulties by developing computing skills through utilising their individual strengths.
- Behavioural or emotional difficulties (including stress and trauma) by developing the understanding and management of their own learning behaviours.
-

Assessment

As in all other subjects, children should be assessed and appraised of their progress in understanding and applying of computing skills. Teacher assessments of computing capability will be recorded throughout the year and reported to parents at the end of each academic year. Staff should keep or save examples of pupils' work and sufficiently detailed records to form a judgement on each pupil's level of attainment at the end of each key stage. Formative assessment occurs on a lesson-by-lesson basis determined by the aims. An online learning management system, Cyber Square is used to assess the students periodically.

Security, Legislation, Copyright and Data Protection

- We ensure that the school community is kept safe by ensuring that:
- The use of ICT and computing will be in line with the school's Acceptable Use Policy (AUP).
- All staff, volunteers and children must sign a copy of the schools AUP.
- Parents are made aware of the AUP at school entry.
- All children are aware of the school rules for responsible use on login to the school network and will understand the consequence of any misuse.
- Reminders for safe and responsible use of ICT and computing and the Internet will be displayed in all areas.

- Software/apps installed onto the school network server must have been vetted by the teacher for suitable educational content before being purchased and installed. No personal software is to be loaded onto school computers. Further information can be found in the school's Data Protection policy.

Teaching and Learning

The schools Scheme of Learning is based on the CBSE Curriculum guidelines. All units of teaching and learning are differentiated. Digital projectors are positioned in all classrooms and are used as a teaching and learning resource across the curriculum.

Across Grade 1 to Grade 12, our children will use technology to:

- Learn Programming by, program on screen, through animation, develop games (simple and interactive) and to develop simple mobile apps.
- Develop their computational thinking through filming, exploring how computer games work, finding and correcting bugs in programs, creating interactive toys, cracking codes and developing project management skills.
- Develop computing creativity by taking and editing digital images, shooting and editing videos, producing digital music, creating geometrical art and creating video and web copy for mobile phone apps.

Teacher's planning is differentiated to meet the range of needs in each class. A wide range of teaching and learning styles are employed to ensure all children are sufficiently challenged. Children may be required to work individually, in pairs or in small groups according to the nature of the task. Different outcomes may be expected depending on the ability and needs of the individual child.

Internet Safety

Internet access is planned to enrich and extend learning activities across the curriculum. However, we have acknowledged the need to ensure that all pupils are responsible and safe users of the Internet and other communication technologies both in school and outside. An AUP for Internet Usage is developed and students are made aware of the same.

Monitoring

Monitoring termly enables the HOD to gain an overview of Computing and ICT teaching and learning throughout the school. This will assist the school in the self-evaluation process identifying areas of strength as well as those for development. In monitoring the quality of Computing and ICT teaching and learning, the HOD will:

- Observe teaching and learning in the classroom.
- Hold discussions with teachers and children.
- Analyse children's work
- Examine plans to ensure full coverage of the Computing and cross-curricular ICT requirements.