CYBER SAFETY AND SECURITY POLICY

2022-2023

HABITAT SCHOOL
AL JURF, AJMAN

Creation date: 20/5/2014
Last amendment date: 26/4/2022
Next review date: April 2023

ONLINE SAFETY GROUP AY 2022-23

SL.NO	Role	Name	Designation
1	Governor	Mr. Wasim Yousuf Bhatt	Dean of Academics
2	Chairman/Child Protection Officer	Mr. Bala Reddy Ambati	Principal
4	Senior Leadership Team	Mr. Suresh Sukumar	Vice principal.
		Ms. Saima Khan	Junior School Head
5	Online Safety Leader	Mr. Ameerudheen Puthan Peedkal Hamza	IT teacher
6	Social Worker	Ms. Sasneem Sanoop	Head of Counselling Department
7	Technical Support	Mr. Bone R	IT Support Admin
8	ICT Teacher	Mr. Faizal	Head of Computer Department
10	Teacher Representative	Ms Renjana K S	Cycle 1
		Ms. Juliet Vergina	Cycle 2
		Ms. Lamiya Abdul Salam	Cycle 3
11	Student Representative	Syeda sidra naaz	Grade 12A
		Krishna pandit	Grade 12 P
		Rudraksh	Grade 10 P
		Nevit Jacob Punnoose	Grade 8 M
		Romaiysa Khattak	Grade 7 C
		Zain Bilgrami Hasan Imad Bilgrami	Grade 6 T
		Jochebed skariya Shaji	Grade 5 D
13	Parent council representative	Sijesh Sidharthan	Grade - 3.A Student Reg No - 13801 Student Name- DIYA K
		Nisamidhin P	Grade - 6.E Student Reg No - 3654 Student Name- JAZA FATHIMA
		Anoop J.S	Grade - 7.P Student Reg No - 0460 Student Name- ADVAITH ANOOP+
		Rajesh	Grade - 10.M Student Reg No - 4899 Student Name- REVIN RAJESH
		Arul Das. S	Grade - 12.M Student Reg No - 2589 Student Name- KRISHNAN ARULDAS

Online Safety Group terms of reference were approved by the Governing body of the school on	Date: 10/03/21
The Implementation will be monitored by the	Principal
Monitoring will take place at regular intervals	Term
Review of the policy	Annually
Next anticipated Review date	April 2023

PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Full Governing Body.

Members of the Online Safety Group will assist the Online Safety Lead with:

- The production/review/monitoring of the school Online Safety Policy/documents.
- The production/review/monitoring of the school filtering policy and requests for filtering changes.
- Mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth, and progression
- Monitoring network/internet/filtering/incident logs
- Consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring improvement actions.

MEMBERSHIP

The online safety group comprises

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff members
- Support staff members
- Online safety leader/ Social worker
- Governor
- Parent/Carer
- ICT Technical Support staff
- Student/pupil representation – for advice and feedback. Student/pupil voice is essential in the make-up of the online safety group, but students/pupils would only be expected to take part in committee meetings where deemed relevant.

- Other people may be invited to attend the meetings at the request of the Chairperson 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.
- Meetings shall be held termly for a period of up to 1.5 hours, depending on needs. A special or immediate meeting may be called when and if deemed necessary.

ROLES AND RESPONSIBILITIES

Governor

- Hold regular meetings with the School Online Safety Lead
- Maintains attendance at Online Safety Group meetings
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant meetings of Governors/Directors/ of Habitat Group

Principal and Senior Leaders

- The Principal has overall executive responsibility and has a duty of care for ensuring the safety (including E-Safety) and welfare of the members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Principal and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. They should also be aware of any relevant local regulations or any overarching regulations that pertain to the organization to which the school belongs
- They are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- They should ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Leader (OSL)

- Lead the Online Safety Group (OSG) of the school.
- Hold and host OSG meetings once in a term and as required in the occurrence of online safety incidents.
- Takes a day to day responsibility for online safety issues and has a leading role in reviewing the school's online safety policies/documents
- Ensure that all staff is aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Organize regular training and advice for staff and parents.
- Liaises with school technical staff
- Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meet regularly with Online Safety Governor/Principal/OSG to discuss current issues, review incident logs, and filter/change control logs
- Report regularly to the Senior Leadership Team.
- Equip (i.e. train) children to stay safe online, both in school and outside of school
- Record online safety incidents and actions are taken, in accordance with the school's normal child protection mechanisms.

Child Protection Officer

Should be trained in Online 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 online contact with adults/strangers
- Potential or actual incidents of grooming
- online-bullying

Social worker:

- promote awareness on all forms of bullying for students, parents, and staff members.
- hold a national anti-bullying week program.
- maintain and review behavior management policies.
- handle disciplinary and e-safety-related issues and maintain records of the same.
- follow the policies of the school and MOE behavior policy when dealing with e-safety cases.
- monitor the behavior scores obtained by the students.

Technical Staff/ IT Advisors

- The Co-coordinator for ICT / Computing is responsible for ensuring:
- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any KHDA / other relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- They have to keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Regularly monitor the use of the networks/internet/digital technologies in order that any misuse/attempted misuse can be reported to the Principal and Senior Leaders; Online Safety Lead for investigation/action/sanction.
- Other responsibilities are mentioned in the school technical security policy

Teaching & Supporting Staff Representatives

Staff are responsible for ensuring that:

- They have up-to-date awareness of e-safety matters and of the current school / academic e-safety policy and practices.
- They have read, understood, and signed the Staff Acceptable Use Policy/ Agreement (AUP).
- They report any suspected misuse or problem to OSL for investigation/action/sanction.
- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the e-safety and acceptable use policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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.
- 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.

Student Representative

- Are responsible for using the school digital technology systems in accordance with the Student/Pupil Acceptable Use Agreement
- 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 online bullying.
- should understand the importance of adopting good online safety practices when using digital technologies out of school and realize that the schools' Online Safety Policy covers their actions out of school if related to their membership in the school

Parent Representative

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' newsletters, letters, websites, social media, and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practices and follow guidelines on the appropriate use of

- digital and video images taken at school events
- and access to parents' sections of the website/Learning Platform and online student/pupil records

Visitors/ Community Users

Visitors/ Community Users, who access school systems/ website as part of the wider school provision are expected to read, understand and sign a Visitors Acceptable Use Policy – Agreement before being provided with access to school systems

CYBER SAFETY AND SECURITY

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 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.

Objectives

- To enable the students to browse the internet safely and understand the importance of using secure connections.
- Inform the students and parents about the protective and safety measures in their use of technology, to be aware of Cyberbullying.
- 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

- 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 letters, 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.

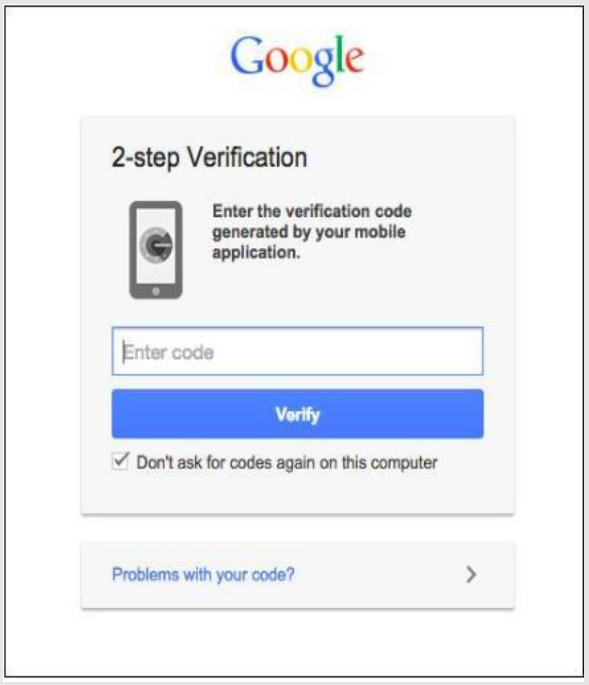
The DO'Ts in the use of Online Technology and Electronic

- Don’t share your mobile number or parent’s mobile number.
- Don’t share your address/location.
- Don't share your personal information: real name, date of birth, etc. unnecessarily.
- Don’t share bank account numbers or credit card numbers of your parents.
- Don’t share your Social Security number /Emirates ID.
- Don’t share your Passwords.
- Don't send your pictures to unknown persons or share them on social media.
- Don't open emails and attachments from strangers.
- Don‘t respond to any suspicious email, instant message or web page asking for personal information.
- Don't enter a password when someone is sitting beside you as they may see it.
- Don't save your username and password on the browser.
- Don't steal other‘s information.
- Don‘t access or use files without the permission of the owner.
- Don't copy software which has copyright without the author‘s permission.
- Don't bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.
- Don't use someone else‘s password even if it is shared with you.

- Don't log in as someone else to read their emails or mess with their online profiles.
- Don't attempt to infect or in any way try to make someone else's computer unusable.
- Don't meet unknown (even if they are known only through online interaction) people alone; always inform your parent.
- Don't open or download any attachments from an unknown source as they may contain viruses.

Tips for safe internet browsing

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



3. Customize your security settings. You can also make a browser more secure by customizing it through its preferences or settings menu.
4. Confirming site's security (https vs http) Check for the Secure as shown on the address bar (Chrome).

5. Backup your data. This means finding a way to copy your information to a safe place so that you don't rely on your computer's hard disk alone.
6. Avoid clicking on links if possible from messages or chats. Viruses spread easily through links in instant messages and email attachments.
7. Bookmark important sites

   If there are sites you visit regularly, it's a good idea to bookmark them in your browser.

Bookmarked addresses take you to the same site every time.

Cyber safety Challenges - Related Terms

- **Cybercrimes** are offenses that may be committed against individuals, companies or institutions by using computers, internet or mobile technology. Cybercriminals use platforms such as social networking sites, emails, chat rooms, pirated software, websites, etc., to attack victims. Children are also vulnerable to various types of cybercrimes.
- **Cyber grooming** is growing as one of the major cyber threats faced by children and teenagers. It is a practice where someone builds an emotional bond with children through social media or messaging platforms with an objective of gaining their trust for sexually abusing or exploiting them. The cyber groomers can use gaming websites, social media, email, chat rooms, instant messaging, etc. by creating a fake account and pretending to be a child or having the same interests as the child.
- **Cyberbullying** 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 Cyberbullying and will take actions as per the national guidelines and laws in case such incidents occur and are reported.

Consequences of Cyberbullying

It can lead to both civil and criminal cases.

CIVIL LAWS

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

CRIMINAL LAWS

- Criminal laws can lead to the arrest and offenders can be put in jail and get fines as well. Using the internet for the following purposes will attract criminal cases in many countries.
- Hate or bias crimes.
- Making violent threats to people or their property.
- Engaging in coercion. Trying to force someone to do something they don't want to do.
- Making harassing telephone calls, sending obscene text messages, and stalking.
- Sexual exploitation and sending sexual images of children under 18 years of age.
- Taking a photo of someone in a place where privacy is expected (locker room, bathroom, etc.) and exploiting it on the internet.

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

If you feel that you are being Cyber Bullied

- Ignore.
- Tell someone.
- Just let a trusted adult know what's going on. The worst thing you can do is to keep it to yourself. Remember, it's not your fault!
- Do not instigate.
- If someone is sending you hurtful messages or posting mean pictures, they're doing it to get an emotional response from you. Don't give them one! Don't respond OR retaliate. This will only encourage them to take it further.
- Block them. If it's on Facebook or another website that allows you to block the person or leave the chat room, then do it!
- Be open to parents about your online identity and image.
- Tell your parents what you do online in general.
- Never indulge in cyber bullying yourself.

How can I use cyber platforms safely?

- Follow the cyber safety guidelines properly.
- Safeguard your device and online accounts.
- Don’t get involved in any kind of improper cyber behavior, even for fun.
- If you face any challenge online, immediately inform your parents 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 offenses.

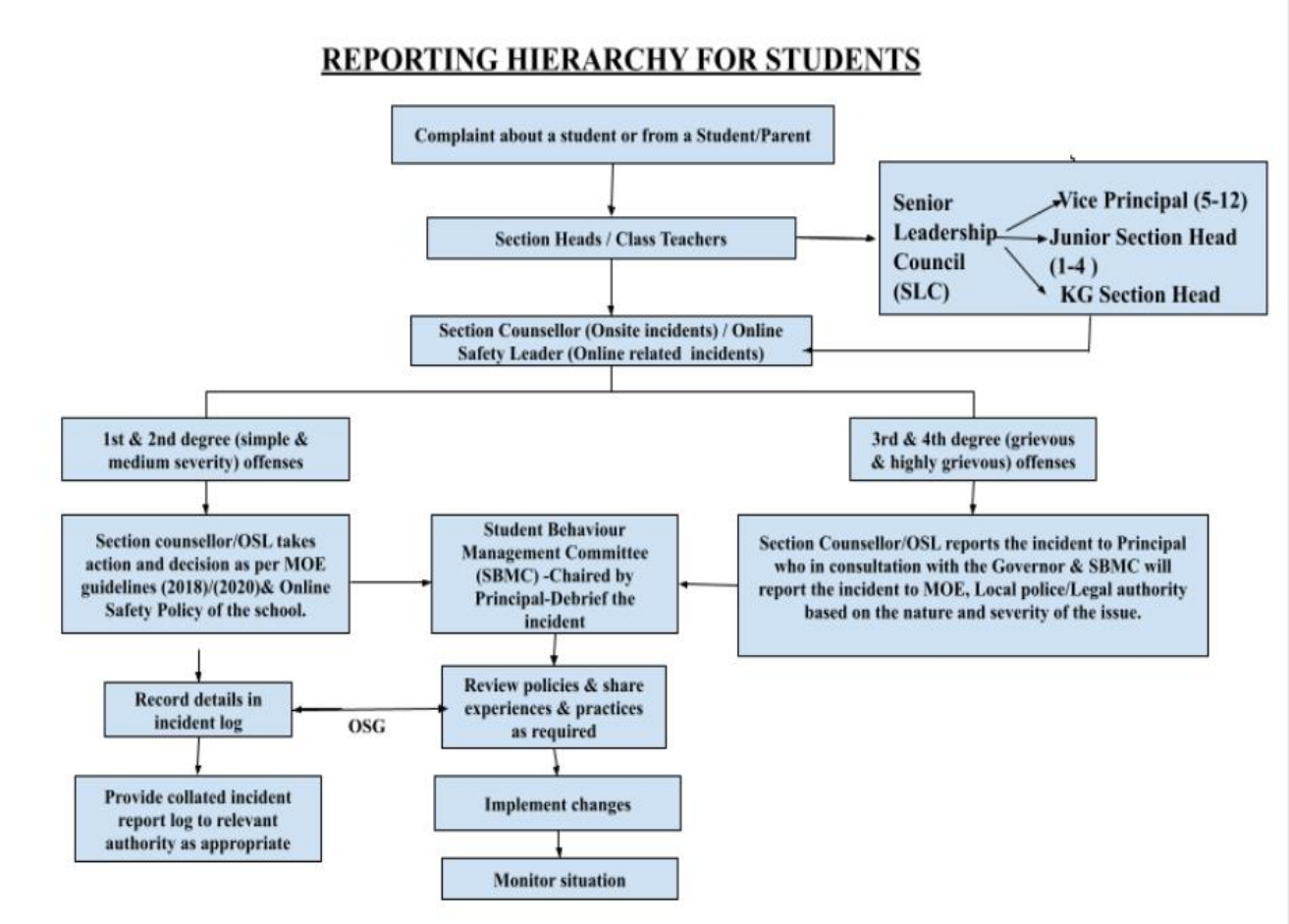
Reporting

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?

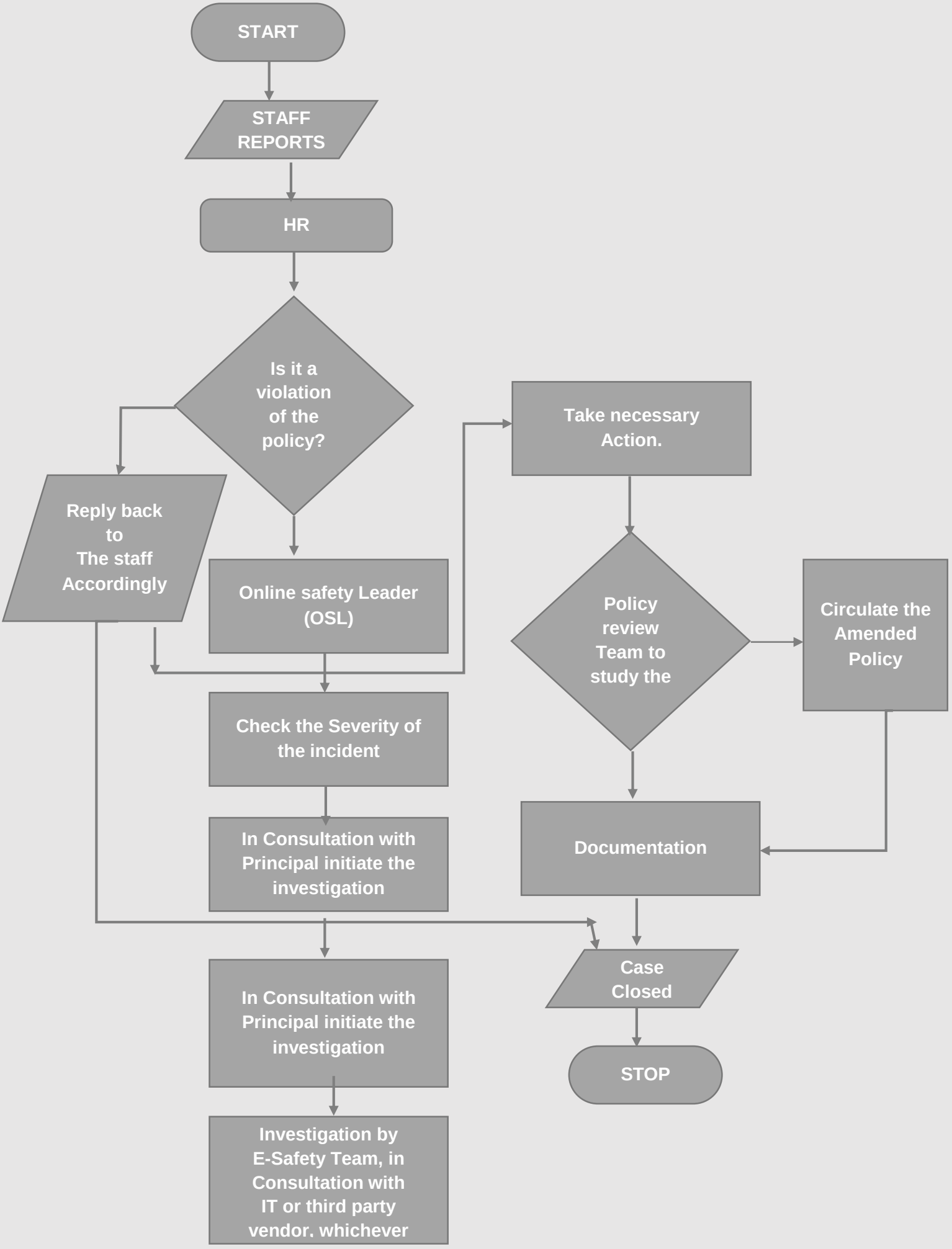
- Share with your parents or elders in the family
- You can ask your parents to write a mail to the Online Safety Leader at osl@ajm.habitatschool.org
- Ask your parents to contact the section head of your respective section. The contact details are given below.

Name: Ms. NishaThomas (Grade 1)	Contact: g1.sh@ajm.habitatschool.org
Name: Ms. Shaila Ahmed Mumtaz Ahmed (Grade 2)	Contact: g2.sh@ajm.habitatschool.org
Name: Mr. Mujbeer K (Grade 3-4)	Contact: g3-4.sh@ajm.habitatschool.org
Name: Mr. Vijeshkumar K (Grade 5-8 Boys)	Contact: g5-8b.sh@ajm.habitatschool.org
Name: Ms. Ayesha (Grade 5-8 Girls)	Contact: g5-8g.sh@ajm.habitatschool.org
Name: Ms. Sajir K (Grade 9-12 Boys)	Contact: g9-12b.sh@ajm.habitatschool.org
Name: Ms. Fatima Sayeeda (Grade 9-12 Girls)	Contact: g9-12g.sh@ajm.habitatschool.org
Name: Ms. Tanzeem Shabir (KG)	Contact: kg.sh@ajm.habitatschool.org

BEHAVIOUR REPORTING HIERARCHY FOR STUDENTS



BEHAVIOUR REPORTING HIERARCHY FOR STAFF



PASSWORD POLICY

Introduction

Effective password management will protect Habitat 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 passwords are the front line of protection for user's accounts. A poorly chosen password may result in the compromise of Habitat's entire network. The purpose of this policy is to provide standards for defining domain passwords to access Habitat IT resources such as email, academic and administrative applications, computing labs and School-owned computer systems for protecting Habitat 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 Habitat School, and shall govern acceptable password use on all systems that connect to the Habitat School network or access or store Habitat School's data.

Policy Password Creation

1. All user and admin passwords must be at least [8] characters in length. Longer passwords and passphrases are strongly encouraged.
2. Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
3. Passwords must be completely unique, and not used for any other system, application, or personal account.
4. Default installation passwords must be changed immediately after installation is complete.

Password Aging

User passwords and system-level passwords must be changed every [6] months. Previously used passwords may not be reused.

Password Protection

1. Passwords must not be shared with anyone (including coworkers and supervisors), and must not be revealed or sent electronically.
2. Passwords shall not be written down or physically stored anywhere in the office.
3. When configuring password "hints," do not hint at the format of your password (e.g., "zip + middle name")
4. User IDs and passwords must not be stored in an unencrypted format.
5. User IDs and passwords must not be scripted to enable automatic login.
6. "Remember Password" feature on websites and applications should not be used.
7. All mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

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 Habitat School 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

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customized 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 program. (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 miss-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 the School network.
- Arts and culture
- Education
- Health and wellness
- News and media
- Sports
- Information and computer security
- Information technology and 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 to 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 Habitat'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 Habitat's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Habitat's direct control to backup, store, and otherwise access Habitat data of any type must adhere to Habitat-defined processes for doing so.

POLICY

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 items is prohibited.

Habitat 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 Habitat School and the device remains the sole property of Habitat 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. Habitat 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.

DATA PROTECTION POLICY

Introduction

Habitat 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.

Scope and 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.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

POLICY

All student, employee, and organization data (Habitat Schools Data) is the property of the Habitat School.

If data on the school’s systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgment when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non- school system any information that is designated as confidential, or that they should reasonably regard as being confidential to the school, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with the school’s safe password policy.

Habitat School Data should not be shared with a third party, including parents or community residents, unless authorized to do so in the performance of their regular duties.

Users who are supplied with computer equipment by the school are responsible for the safety and care of that equipment, and the security of software and data stored on other school systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

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

Habitat School critical servers are backed up automatically by Imperils 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 Habitat 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

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.

Data protection Officer and Information asset owner of Habitat School, Al Jurf: Mr. Boney R

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

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 behavior
- 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 do 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:

1. Legal entities like MOE, CBSE etc.

2. 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 do we collect information?

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

We always ensure only authorized 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 parents/careers permission before taking images or videos or students/staff. In case of sharing the images of students 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/careers 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/careers 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 colors 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/career/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 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/career/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 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 forwarded 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 the CBSE curriculum. High quality teaching of Computing, from Grade 1 to Grade 8, utilizes 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.

Aim of the Policy

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 behaviors.
- 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 programs, 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 utilizing their individual strengths.
- Behavioral or emotional difficulties (including stress and trauma) by developing the understanding and management of their own learning behaviors.

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 judgment 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

- 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 school's 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.
- Analyze children's work
- Examine plans to ensure full coverage of the Computing and cross-curricular ICT requirements.