CYBER SAFETY AND SECURITY POLICY 2023-2024

HABITAT SCHOOL
AL JURF, AJMAN

Creation Date: 20/05/2014

Last Amendment Date: 26/4/2023

Next Review Date: April 2024

Policy Committee Members

- Dean Academics
- Principal
- Vice Principal
- KG Section Head
- Junior School Head
- Administrative Officer
- Head Of Counseling Department
- Social worker
- Head of Computer Department
- School IT Administrator
- Software Analyst- Corporate

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	Online Safety Group Members, Student Behavior Management Committee
Monitoring will take place at regular intervals	Term
Review of the policy	Annually
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.

Introduction

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

Cyber safety is the safe and responsible use of information and communication technology. It is not just about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette). This policy covers all aspects of the technology usage of students regarding the school context both inside the school premises and in the 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 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 etiquette of electronic communication.

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

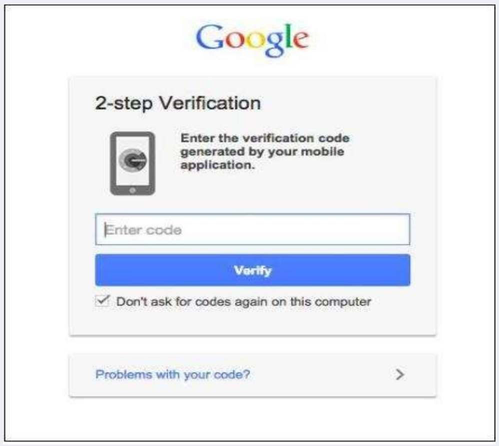
- Respect the privacy of others.
- Report and flag content that is abusive or illegal.
- Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.
- Report online bullying immediately to the teacher and parents/ or someone whom you trust.
- 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.
- Donʿt 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 otherʿs information.
- Donʿt access or use files without the permission of the owner.
- Don't copy software which has copyright without the authorʿs permission.
- Don't bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.
- Don't use someone elseʿs 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 elseʿs computer unusable.
- Donʿt 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.



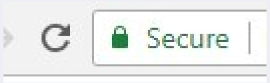
Google

2-step Verification

Enter the verification code generated by your mobile application.

Enter code
Verify
☑ Don't ask for codes again on this computer
Problems with your code? >

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, the 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.

- **Cyberbullying** means using the internet or mobile technology to intentionally harass or bully someone by sending rude, mean, or hurtful messages, comments, and images/videos. A cyberbully 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 action 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 cyberbullied

- 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 cyberbullying 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

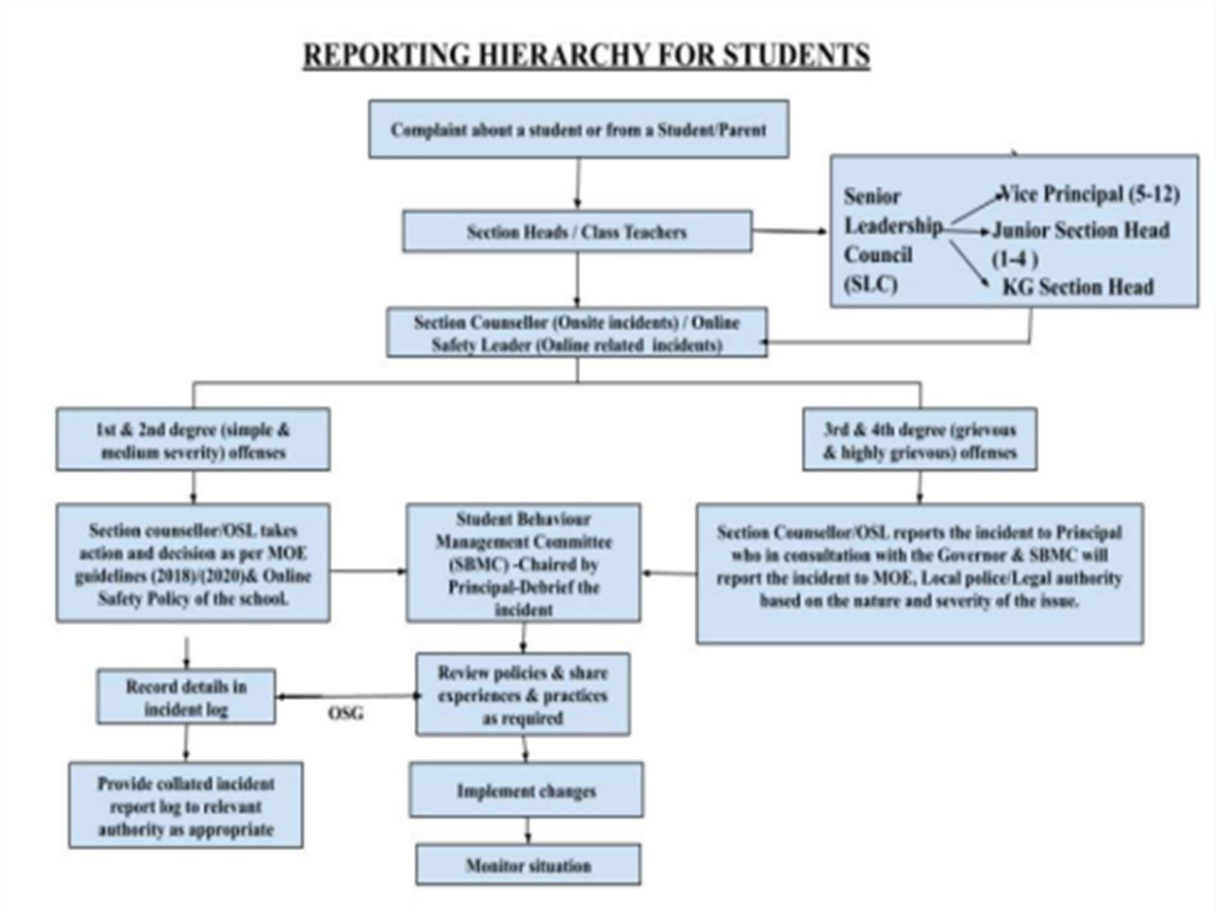
If a student faces an uncomfortable situation online, specifically if someone is threatening or bullying online, especially during Online Learning sessions, who should be contacted?

- Share with your parents or elders in family
- Report to the school Online Safety Leader (OSL), Ms. Sasneem Sanoop at osl@ajm.habitatschool.org

- Other Contacts:

Name of Section Heads	**Section**	**Email id**	**Contact no:**
Ms. Tanzeem Shabir	KG	kg.sh@ajm.habitatschool.org	0543077283
Ms. NishaThomas	Grade 1	g1.sh@ajm.habitatschool.org	0543078033
Ms. Shaila Ahmed	Grade 2	g2.sh@ajm.habitatschool.org	0543077379
Mr. Mujbeer K	Grade 3 & 4	g3-4.sh@ajm.habitatschool.org	0543077635
Mr. Suresh Sukumar	Grade 5-8 Girls	vp@ajm.habitatschool.org	054542705
Mr. Vijesh Kumar	Grade 5-8 Boys	g5-8b.sh@ajm.habitatschool.org	0569925527
Ms. Fathima Sayeeda	Grade 9-12 Girls	g9-12g.sh@ajm.habitatschool.org	0543077642
Mr. Sajir Kanjirampara	Grade 9-12 Boys	g9-12b.sh@ajm.habitatschool.org	0569945034

Reporting procedure for student related online incidents:


REPORTING HIERARCHY FOR STUDENTS
Complaint about a student or from a Student/Parent
Section Heads / Class Teachers
Senior Leadership Council (SLC)
Vice Principal (5-12)
Junior Section Head (1-4)
KG Section Head
Section Counsellor (Onsite incidents) / Online Safety Leader (Online related incidents)
1st & 2nd degree (simple & medium severity) offenses
3rd & 4th degree (grievous & highly grievous) offenses
Section counsellor/OSL takes action and decision as per MOE guidelines (2018)/(2020)& Online Safety Policy of the school.
Student Behaviour Management Committee (SBMC) -Chaired by Principal-Debrief the incident
Section Counsellor/OSL reports the incident to Principal who in consultation with the Governor & SBMC will report the incident to MOE, Local police/Legal authority based on the nature and severity of the issue.
Record details in incident log
OSG
Review policies & share experiences & practices as required
Provide collated incident report log to relevant authority as appropriate
Implement changes
Monitor situation

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 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

- Governor
- Child Protection/Safeguarding officer
- Senior Leaders
- Online safety leader/ Social worker
- ICT Technical Support staff
- Teaching staff members
- Parent Council Representatives
- Student representatives - 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.

Online Safety Group Committee Members

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	Ms. Sasneem Sanoop	Head of Counseling Department
6	Social Worker	Mr. Stebin Manoj	Counselor, 5-12 Boys
7	Technical Support	Mr. Boney R	IT Support Admin
8	ICT Teacher	Ms. Deepthi Das	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	Bibi Aysha	Grade 11 A
		Abbas Abdul Khadeer	Grade 11 P
		Muhammed Anas Manu S	Grade 11 M
		Vismaya Rajesh	Grade 10 A
		Ayska Kausar	Grade 9 D
		Ashwin Kumar Senthil Kumar	Grade 9 S
		Sarrinah Sameer	Grade 9 E

13	Parent council representative	Sivanandan	Grade - 4.Q Student Reg No - 19813 Student Name- KAASHINADH ARUN
		Mr. Nsdeem Ahamed	Grade - 7.M Student Reg No - 19917 Student Name- AADIL AHAMED
		Anoop J.S	Grade - 8.T Student Reg No - 0460 Student Name- ADVAITH ANOOP
		Noushad KT	Grade - 9.S Student Reg No - 10141 Student Name- AASHIN NOUSHAD
		Krishna Kumar.	Grade - 10. P Student Reg No - 9636 Student Name- ESHWAR KRISHNA

- 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 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.

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 relevant meetings of Governors/Directors/ of Habitat Group.

Child Protection Officer (CPO) - Principal

- 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 being the CPO of the school, should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from
- the sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying
- 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 to raise awareness about the policies and their implementation

Senior Leaders

- Senior Leaders include KG Section Head, Junior School Head, Vice Principal, and Administrative officer.
- The Senior Leaders 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/ student. They should also be aware of any relevant local regulations or 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 are also responsible for ensuring that students are taught through orientation sessions how to use ICT tools such as the internet, email and social networking sites, safely and appropriately.
- 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 Leaders will receive regular monitoring reports from the Online Safety Lead.

- They 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.

Online Safety Leader (OSL)

- Lead the Online Safety Group (OSG) of the school.
- Hold and host OSG meetings once a term and as required in the occurrence of online safety incidents.

- Take day-to-day responsibility for online safety issues and have 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 create 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 taken, by the school's normal child protection mechanisms.

Social worker:

- Promote awareness of 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 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 regularly and its implementation is not the sole responsibility of any single person.
- They have to keep up to date with online safety technical information 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 so that any misuse/attempted misuse can be reported to the Principal and Senior Leaders the 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 about 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

- They are responsible for using the *school* digital technology systems by the Student Acceptable Use Agreement
- They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They need to understand the importance of reporting abuse, misuse, or access to inappropriate materials and know-how to do so
- They 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 online bullying.
- They 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 appropriately. 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 are followed when using the school digital technology systems under the Acceptable Use Policy guidelines and guide the children appropriately.

- 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 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.

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, and 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 passwords 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, website, Learning Management System, Orisson portal.
- Parent's 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 training will be offered as follows:

- A planned programme of formal E-Safety training will be made available to staff for the new academic year in collaboration with NOS. It is expected that OSL will identify E-Safety as a training need within the performance management process.
- All new staff will receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies.
- This E-Safety policy and its updates are presented to and discussed with staff.
- All staff are required to undertake training through the National Online safety platform.
- The E-safety Leader provides advice/guidance/training as required to individuals.

Training – OSL & OSG

- Take part in E-Safety awareness sessions or trainings offered in the school.
- Participate in external workshops/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 in the coding club.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request 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 online 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:

Effective password management will protect Habitat School's data and reduce the risk of unauthorized application 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 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 Habitat School network or access or store Habitat School's data.

Policy

- These statements apply to all stakeholders (Staff, Students, Parents, and Vendors) of Habitat School.
- All school networks and systems will be protected by secure passwords.
- All users are clearly defined with 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 a responsibility for 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 the IT Administrator who will keep an up-to-date record of users and their usernames

Password Creation

- 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, numbers, 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's account is compromised.

- Passwords must not contain any personal information about the user that might be known by others.
- 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.
- The administrator has an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration is given to 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 are only used to recover or revoke access. Other administrator accounts cannot delete this account.

Password Aging

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

Password Protection

- Default installation passwords must be changed immediately after installation is complete.
- Passwords must not be shared with anyone, and must not be revealed or sent electronically.
- Passwords must not kept in writing or electronically which can be accessible by others.
- User IDs and passwords must not be stored in an unencrypted format.
- User IDs and passwords must not be scripted to enable automatic login.
- The “Remember Password” feature on websites and applications should not be used.
- All mobile devices that connect to the school network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.
- Records of learner usernames and passwords for younger students are securely kept which is accessible only by the IT administrator.
- Students will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.
- Any digitally stored administrator passwords are 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 knows the password.
- Wherever user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users are allocated by the administrator. This password should be temporary and the user should be forced to change their password on the first login.
- Where automatically generated passwords are not possible, the 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 are authenticated by the administrator to ensure that the new password can only be passed to the genuine user.
- Suitable arrangements are provided to visitors for appropriate access to systems that 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's imperative to educate users about the significance of maintaining secure passwords and the potential dangers associated with unauthorized access and data loss. This applies even to the youngest users, emphasizing the importance of responsible password management. By ensuring that all stakeholders understand how passwords can be compromised, we empower them to make informed decisions and adopt secure practices to safeguard sensitive information effectively.

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

- During induction
- Through the school’s online safety policy and password security policy
- Acceptable use agreement

Students 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 maintain comprehensive records encompassing

- User Ids and requests for password changes
- User logins
- Any security incidents pertinent 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. The school must have a filtering policy to manage the associated risks and to provide preventative measures that 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, 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 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 before changes are 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 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 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

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, and briefings.

Parents will be informed of the school’s filtering policy through the Acceptable Use Agreement and online safety awareness sessions/newsletters 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 miscategorized, 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 that 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 those 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
- 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 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 based on 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 the 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 websites in addition to the 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 comply 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, smartphones 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

The school has implemented technical solutions to ensure the safe and responsible use of mobile technology for both school-issued and personal devices.

- Access control measures are tailored to meet user requirements, including internet-only access and shared folder network access.
- Broadband performance and capacity have been optimized to support core educational and administrative activities, even with an increased number of connected devices.
- Filtering is enforced on all mobile technologies to regulate internet connections, and attempts to bypass these measures are prohibited.
- Clear exit processes are in place for devices no longer in use at school locations or by authorized users. Routine and proactive monitoring ensure adherence to safety protocols.
- Regarding personal devices, users assume full responsibility and liability for any loss or damage resulting from bringing their devices onto school premises. The school does not accept responsibility for lost, stolen, or damaged devices while on school grounds or during school activities, and recommends purchasing insurance for coverage outside the home.
- Users are encouraged to make their devices easily identifiable and to set passcodes or PINs for added security.

- The school is not responsible for day-to-day maintenance or upkeep of personal devices, including charging, software updates, or hardware issues.
- Users are expected to adhere to current Acceptable Use Agreements, including refraining from using personal devices during tests or exams. Visitors receive guidance on permitted mobile technology use per local safeguarding arrangements.
- Users are responsible for keeping their devices up to date with software, security, and app updates.
- Personal devices must be charged before bringing them to school, as charging during the school day is not permitted. Devices must remain in silent mode on school premises and school buses.
- School-provided devices are intended for learning support, and pupils/students are expected to bring devices as required.
- Staff-owned devices should not be used for personal purposes during teaching sessions, except in exceptional circumstances. Printing from personal devices is not supported.
- Confiscation and searching of devices suspected of unauthorized use are within the school's rights.
- Users are prohibited from altering settings that disrupt device functionality.
- School-installed software must remain accessible and in usable condition, with periodic checks to ensure compliance.
- The school ensures that devices contain the necessary apps for school work. School-owned apps remain the property of the school and are inaccessible to students once they leave. Users are reminded to adhere to app age limits and usage terms and conditions.
- Users must obtain permission before photographing individuals and should only take necessary images or videos.
- Devices may be used in lessons under teacher direction.

Employees are expected to use good judgment when engaging in personal calls, sending/receiving text messages, and/or Internet usage on their mobile devices 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 school-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 the 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 of the policies above.

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

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 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 similar items commonly understood to be covered by this term.

POLICY

All student, employee, and Habitat Schools Data is the property of the Habitat School.

If data on the school’s systems is classified as confidential this should be 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.

Habitat Schools 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.

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.

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

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 of a combination of simpler words and must ensure all passwords comply with the school's safe password policy. Users must keep passwords secure, never share them with anyone and not allow others to access their accounts.

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.

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.

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 offsite. 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 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 Iperius at 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. The 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 to secure the internet and email communication. The firewall works to prevent users from watching unintended materials, torrent downloading etc. As per the levels set by the administration, some of the users have 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 organization or authorized 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

BACKUP AND DISASTER RECOVERY POLICY

Habitat School critical servers are backed up automatically by Imperis at 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. The 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 to secure the internet and email communication. The firewall works to prevent 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 organization or authorized 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 authorization.

DATA BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized 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 has a 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 for non-recurrence and further awareness raising

Everyone in the school has the responsibility of handling protected or sensitive data safely and securely.

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

ENFORCEMENT

It is the responsibility of the end user to ensure enforcement of the policies above. All concerns, questions, and suspected, 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**

REVIEW

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

CONTACT

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

FAIR PROCESSING NOTICE

What is the purpose of this Notice?

Habitat 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 types of information that we collect include:

- Names, contact details including emergency contacts
- Characteristics such as language, nationality, and 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 the registration process as per MOE requirements
- To support children with medical conditions, allergies and Special Education Needs 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 that 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 cover 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 of students/staff. In case of sharing the images of students or staff on public media, only first names 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 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/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 access to this form.
- The form is stored in 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 copies 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, and 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.
- The 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.

Reuse of Photos/Videos

No students, teachers, or staff are allowed to download or copy the photos or videos published on the school's official pages for their personal use with or without the parent's consent. Such usage will be a violation of the Data Protection legislation. However, they are allowed to share the posts 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 Habitat 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 can 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 Grades 1 to Grade 8. For Grades 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 about 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.

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 cohesively and consistently.
- Access to computers within the class or in designated communal areas.
- Experience in 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 lives as active participants in a digital world.

OBJECTIVES

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 lives 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's 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 utilizing their strengths.

- Behavioral or emotional difficulties (including stress and trauma) by developing the understanding and management of their 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 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 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 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 consequences 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 Grades 1 to Grade 12, our children will use technology to:

- Learn Programming by, program on screen, through animation, develop games (simple and interactive), and 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.

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

- Governor
- Child Protection/Safeguarding officer
- Senior Leaders
- Online safety leader
- Social worker
- ICT Technical Support staff
- Teaching staff members
- Parent Council Representatives
- Support staff members
- Student representation – for advice and feedback. Student voice is essential in the make-up of the online safety group, but students 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 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

- 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 relevant meetings of Governors/Directors/ of Habitat Group

Child Protection Officer (CPO) - Principal

- 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 being the CPO of the school, should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from
- the sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying
- 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 to raise awareness about the policies and their implementation

Senior Leaders

- Senior Leaders include KG Section Head, Junior School Head, Vice Principal, and Administrative officer.
- The Senior Leaders 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/ student. They should also be aware of any relevant local regulations or 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 are also responsible for ensuring that students are taught through orientation sessions how to use ICT tools such as the internet, email and social networking sites, safely and appropriately.
- 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 Leaders will receive regular monitoring reports from the Online Safety Lead.
- They 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 andguidance relating to the safe and appropriate use of this online facility.

Online Safety Leader (OSL)

- Lead the Online Safety Group (OSG) of the school.
- Hold and host OSG meetings once a term and as required in the occurrence of online safety incidents.

- Take day-to-day responsibility for online safety issues and have 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 create 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 taken, by the school's normal child protection mechanisms.

Social worker:

- Promote awareness of 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 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 regularly and its implementation is not the sole responsibility of any single person.
- They have to keep up to date with online safety technical information 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 so that any misuse/attempted misuse can be reported to the Principal and Senior Leaders the 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

- They are responsible for using the *school* digital technology systems by the Student Acceptable Use Agreement
- They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They need to understand the importance of reporting abuse, misuse, or access to inappropriate materials and know-how to do so
- They 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 online bullying.
- They 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 appropriately. 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 are followed when using the school digital technology systems under the Acceptable Use Policy guidelines and guide the children appropriately.

- 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 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.

CONTACT

If you have any queries or concerns regarding this policy, please contact principal@ajm.habitatschool.org