HABITAT SCHOOL
AL TALLAH, AJMAN,UAE

IT POLICY (2025 - 26)

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.*

SUMMARY	
Updated Date	01-Apr-25
Next Update	01-Apr-26
Review Committee	Dr. HUMA ATHAR VICE PRINCIPAL Dr. UVAIS VALIYANEERILAKKAL ADMIN OFFICER
Approved by	MARIYAM NIZAR AHAMED
	PRINCIPAL
Compiled by	KASHIF MAJEED
	IT SUPPORT

Introduction:

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

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

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

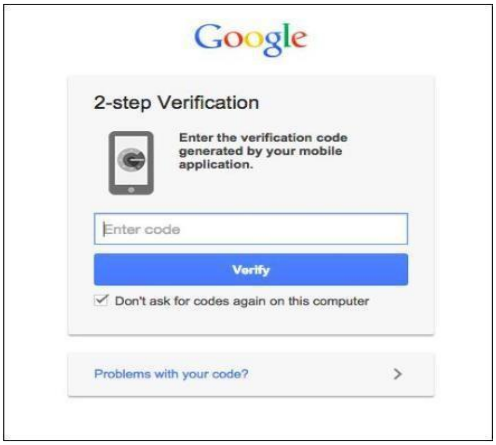
- Respect the privacy of others.
- Report and flag content that is abusive or illegal.
- Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.
- Report online bullying immediately to the teacher and parents/ or someone whom you trust.
- Use a strong and unique password with a combination of numbers, uppercase and lowercase letters, and special characters for each account.
- 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 people or share them on social media.
- Don't open emails and attachments from strangers.
- Don’t respond to any suspicious email, instant message, or web page asking for personal information.
- Don’t enter a password when someone is sitting beside you as they may see it.
- Don't save your username and password on the browser.
- Don't steal other’s information.
- Don‘t access or use files without the permission of the owner.
- Don't copy software which has copyright without the author‘s permission.
- Don't bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.
- Don't use someone else‘s password even if it is shared with you.
- Don't log in as someone else to read their emails or mess with their online profiles.
- Don't attempt to infect or in any way try to make someone else‘s computer unusable.
- Don‘t meet unknown (even if they are known only through online interaction) people alone; always inform your parent.
- Don't open or download any attachments from an unknown source as they may contain viruses.

Tips for safe internet browsing

- Update your browser frequently.
- 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.



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

- 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.
- Avoid clicking on links from messages or chats whenever possible. Viruses spread easily through links in instant messages and email attachments.
- 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 also use platforms such as social networking sites, emails, chat rooms, pirated software, and websites 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 the objective of gaining their trust to sexually abuse or exploit them. Cyber groomers can use gaming websites, social media, email, chat rooms, and instant messaging by creating fake accounts and pretending to be a child or to have the same interests as the child.

- **Cyber bullying** means using internet or mobile technology to intentionally harass or bully someone by sending rude, mean or hurtful messages, comments and images/videos. A cyber bully can use text messages, emails, social media platforms, web pages, chat rooms, etc. to bully others.

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

.

CONSEQUENCES OF CYBER BULLYING

It can lead to both civil and criminal cases.

CIVIL LAWS

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

CRIMINAL LAWS

- Criminal laws can lead to the arrest of offenders, who can be put in jail and fined. Using the internet for the following purposes can attract criminal charges in many countries.
- Hate or biased crimes.
- Making violent threats to people or their property.
- Engaging in coercion. Trying to force someone to do something they don't want to do.
- Making harassing telephone calls, sending obscene text messages, and stalking.
- sexual exploitation and sending sexual images of children under 18 years of age.
- Taking a photo of someone in a place where privacy is expected (locker room, bathroom, etc.) and exploiting it on the internet.
- Taking a photo of someone without their consent and posting publicly.

If you feel that you are being Cyber Bullied

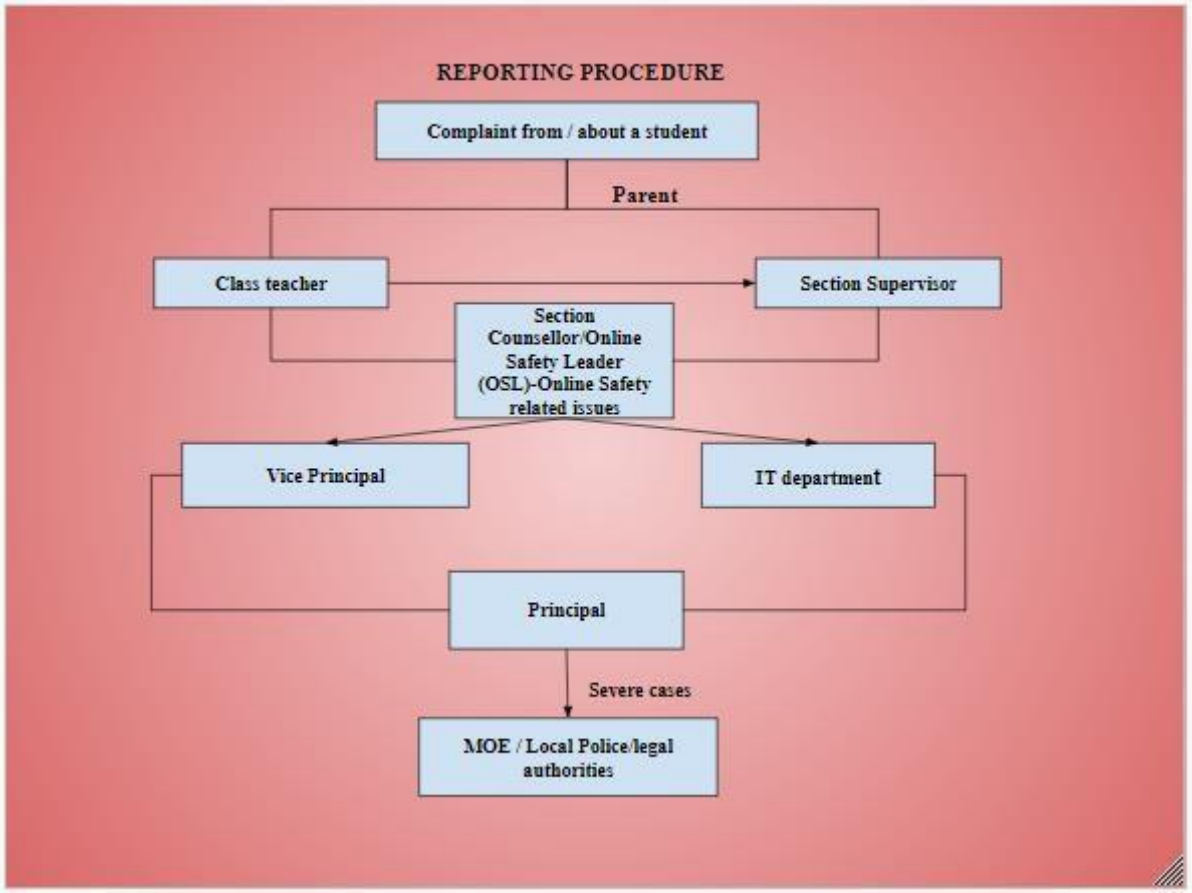
- Ignore.
- Tell someone.
- Just let a trusted adult know what's going on. The worst thing you can do is to keep it to yourself. Remember, it's not your fault!
- Do not instigate.
- If someone is sending you hurtful messages or posting mean pictures, they're doing it to get an emotional response from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

How Can I Use Cyber Platforms Safely?

- ✓ Follow the cyber safety guidelines properly.
- ✓ Safeguard your device and online accounts.
- ✓ Don't get involved in any kind of improper cyber behavior, even for fun.
- ✓ If you face any challenge online, immediately inform your parents or elders so that they can support you and contact the 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- STUDENTS

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?



Hotline Number: 0558875434

PASSWORD POLICY

Introduction:

Effective password management will protect Habitat School's data and reduce the risk of unauthorized applications access. The policy is to establish a secure information technology environment by enforcing the use of strong passwords. Strong and complex 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

Password Creation

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

Password Aging

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

Password Protection

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

Enforcement

It is the responsibility of the end user to ensure compliance with the policies above. This policy is linked to all other policies of the school.

FILTERING POLICY

Introduction

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

Scope

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

Responsibilities

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

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

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

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

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

Policy Statements

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

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

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

Education/Training/Awareness

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

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

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

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

Changes to the Filtering System

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

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

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

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

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

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

Monitoring will take place as follows:

Audit/Reporting

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

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

The school IT department provides an effective filtering system, as a result of which the following categories of websites are, by default, not available to students: -

- **Adult:** content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity.
- **Violence:** content containing graphically violent images, video or text.
- **Hate Material:** content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds.

- **Illegal drug taking and the promotion of illegal drug use:** content relating to the use or promotion of illegal drugs or misuse of prescription drugs.
- **Criminal skill/activity:** content relating to the promotion of criminals 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 preapproval.

Hardware and general service provision:

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

1. A hardware firewall filter is installed which intercepts all Internet traffic leaving and entering the school network and this cannot be circumvented. This firewall appliance is configured for the Global view Internet filtering service. This service is a professional, commercial category-based web filtering solution in use. It uses a category-based system to group web sites in addition to keyword, Content filtering, IP and specific white and blacklist control. School licenses are purchased on a fixed three-year term to ensure continuity of service and the individual firewall is monitored 24/7 with instant notification of any concerns.
2. 2. In addition, IP and URL blacklisting and whitelisting are supported locally, which ensures that any content flagged as undesirable on the network can be disabled immediately.
3. Full access logs are maintained for all traffic and all attempts at access of inappropriate content.

Enforcement

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

MOBILE DEVICE POLICY

Purpose & Scope

The purpose of this policy is to define standards for end users who have legitimate business requirements to use a private or School provided mobile device that can access the school's electronic resources.

This policy applies to, but is not limited to, the use of mobile/cellular phones, laptop/notebook/tablet computers, smart phones and PDAs, and any mobile device capable of storing corporate data and connecting to an unmanaged network, hereinafter referred to as "mobile device."

The goal of this policy is to protect the integrity and confidential data that resides within Habitat's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to Habitat's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Habitat's direct control to backup, store, and otherwise access Habitat data of any type must adhere to Habitat-defined processes for doing so.

Policy

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

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

The use of mobile devices to photograph and/or record confidential information, private information and/or related item is prohibited.

Habitat School will not be liable for the loss of personal mobile devices brought into the workplace.

Any connection to the school's information services must adhere to the Acceptable Use of Technology Policy. Employees may not use any cloud-based apps or backup that allows company related data to be transferred to unsecure parties.

Certain employees may be issued a school owned mobile device. Use of these devices is contingent upon continued employment with Habitat School, and the device remains the sole property of Habitat School. Excessive use of minutes or bandwidth for non-business activity is discouraged and may result in a payroll deduction for personal usage.
Upon resignation or termination of employment, the employee may be asked to produce the mobile device, which will then be reset to factory defaults using 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 compliance with the policies outlined above. Based on the severity of the violation, the following steps will be taken:

First Violation		
Verbal warning by Section Head / HSE		
Ms. Anni M. Jones	Middle Section Head	sectionheadmid@tallah.habitatschool.org
Ms. Neethu Jomon	Primary Section Head	sectionheadpri@tallah.habitatschool.org
Ms. Sheelu Bajpai	KG Section Head	sectionheadkg@tallah.habitatschool.org
Ms. Anjana Geothendran Pillai	Grade 5–12 Girls Section Head	sectionheadgirls@tallah.habitatschool.org
Mr. Anuraj Geetha Sudhakaran	Grade 5–12 Boys Section Head	sectionheadboys@tallah.habitatschool.org
Verbal warning by Section Head / HSE - Non - Teaching Staff		
Mr. Rinu Regi	HSE Officer	sssupervisor@tallah.habitatschool.org
Second Violation		
Memos will be issued by the Principal for teachers and by the Administrative Officer for non-teaching staff.		
Ms. Mariyam Nizar Ahmed	Principal	principal@tallah.habitatschool.org
Mr. Uvais Valiyaneerilakkal	Admin Officer	ao@tallah.habitatschool.org
Third Violation		
Grounds for summary dismissal and cooperation with criminal investigation for any illegal activity		

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 in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

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

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Scope & Objective

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

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

What is Personal Information?

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

Policy

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

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

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

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

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

Habitat 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.

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 only in encrypted folders. Users will be held responsible for the consequences of theft or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

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

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

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

Backup and Disaster Recovery Policy

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

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

Enforcement

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

All concerns, questions, suspected breaches, or known breaches shall be immediately reported to Data Protection Officer.
Data protection Officer and Information asset owner of Habitat School, Assist IT Manager Mr. Boney R

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

FAIR PROCESSING NOTICE

What is the purpose of this Notice?

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

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

What information do we collect?

The types of information that we collect include:

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

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

How 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 on 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: -

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

Who will we share information with?

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

We share information with:

- Legal entities like MOE, CBSE etc.

- Service providers offer learning platforms and communication tools. We select our third-party service providers with care. We provide these third parties with the information necessary to provide the service, and we have an agreement in place requiring them to operate with the same level of care over data protection as we do.

How do we keep your information safe?

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

We always ensure that only authorised persons have access to your information, which means only our employees and vendors, and that everyone with 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 PHOTOGRAPHS AND VIDEOS

Introduction

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

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

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

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

Aim of the Policy

- To enhance the school activities by adding a ray of colours through articles and photos.
- To help parents and the local community to identify and celebrate the schools' achievements.
- To increase pupil motivation and staff morale
- To promote a way of community spirit within the varsity
- To encourage parents and students to share their input 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 at the office of the School Academic Secretary, along with the documents of the students/staff.

- Each form will be kept for two Academic Years and will be disposed of properly (Soft copies will be deleted and hard copy will be shredded) upon the completion of the year/once the student/staff leaves the school. However, the parent/carer/staff is free to change or update the permission at any point in time.

The use of images

- The photos and videos will be used on platforms including the school website and school social media pages, such as 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 and videos.
- Images and videos are stored digitally and shared with the relevant persons via Google folders.
- Images/Videos will be stored for two Academic Years
- Images/Videos will be stored digitally and will be deleted upon the completion of two years.
- In case the student/parent/staff wants to remove a photo that is uploaded online, a request can be forward to the school media coordinator to remove the file.

Re-use of Photos/Videos

No students, teachers, or staff are allowed to download or copy the photos or videos published on the school's official pages for their personal use, with or without parental consent. Such use will be a violation of data protection legislation. However, they are allowed to share the posts or videos as they appear on the official pages.

Concerns

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

COMPUTING AND ICT POLICY

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

The relevance of and the possibilities of emerging technologies thus preparing them for the world of work.

Purpose

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

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

Aims

Computer Science

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

Digital Literacy

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

Information Technology

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

Objectives

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

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

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

It is our policy to ensure that all children, regardless of race, class or gender, should have the opportunity to develop computing and computer science knowledge. We aim to respond to children'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 utilising their individual strengths.
- Behavioural or emotional difficulties (including stress and trauma) by developing the understanding and management of their own learning behaviours

.

Assessment

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

Security, Legislation, Copyright and Data Protection

- We ensure that the school community is kept safe by ensuring that:
- The use of ICT and computing will be in line with the school's Acceptable Use Policy (AUP).
- All staff; volunteers and children must sign a copy of the schools AUP.
- Parents are made aware of the AUP at school entry.
- All children are aware of the school rules for responsible use on login to the school network and will understand the consequence of any misuse.
- Reminders for safe and responsible use of ICT and computing and the Internet will be displayed in all areas.
- Software/apps installed onto the school network server must have been vetted by the teacher for suitable educational content before being purchased and installed. No personal software is to be loaded onto school computers. Further information can be found in the school's Data Protection policy

Teaching and Learning

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

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

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

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

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

ACCEPTABLE USE POLICY

MEMBERS OF THE COMMITTEE

Ms. Mariyam Nizar Ahamed	**Principal**
Dr. Huma Ather	**Vice Principal**
Mr. Kashif	**System Administrator**
Ms.Meenal Umamagesh	**HoD, Computer Science Department**
Mr. Muhammed Saleeque	**Computer Science Department**

SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW

AUP was approved by the Governing body of the school on	01/04/2020
The Implementation of this policy will be monitored by the	Child Protection Team
Monitoring will take place at regular intervals	Annually
Review of the policy	Annually
Last Review Date	10/04/2025
Next anticipated Review date	April 2026

School Acceptable Use Policy

1. Introduction

This is a universal policy that applies to all Users and all Systems. This Acceptable Use Policy (AUP) is designed to protect the school, students, employees, parents and other partners from harm caused by the misuse of our IT systems, internet, and our data. Misuse includes both deliberate and inadvertent actions. The repercussions of misuse of our systems can be severe.

This policy covers only the internal use of the school systems and does not cover the use of our products or services by customers or other third parties. Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases, the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases, local teams should develop and issue users with a clarification of how the policy applies locally.

2. Definitions

"Users" are everyone who has access to any of the school's IT systems. This includes permanent employees and also temporary employees, parents, students, contractors, agencies, consultants, suppliers, customers and business partners.

"Systems" means all IT equipment that connects to the school network or access school applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

3. Scope

This Acceptable Use Policy (AUP) details specific requirements for the use of all computing and network resources at the Habitat School, including electronic and hardcopy data, information, and information assets.

In general, acceptable use means ensuring that the information resources and technology of the University are used for their intended purposes while respecting the rights of other computer users, the

integrity of the physical facilities, the confidentiality of data, information, and information assets, and all pertinent license and contractual agreements.

This policy includes:

- Use of IT system by Staff
- Unacceptable use by Staff
- Acceptable use of IT systems / Internet by students
- Unacceptable use for Students

4. Use of IT Systems by Staff

Everyone who works at the school is responsible for the security of the school's IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager or IT Head. Staff members of the school who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

- All data stored in the school systems is the property of the school. Users should be aware that the school cannot guarantee the confidentiality of the information stored on any school system except where required to do so by local laws.
- The school's systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users own or their colleague's productivity and nor should it result in any direct costs being borne by the school other than for trivial amounts (e.g., an occasional short telephone call).
- The school trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the School's IT systems. If employees are uncertain, they should consult the IT department.
- Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorized access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorized parties.
- The school can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and

- The school reserves the right to regularly audit networks and systems to ensure compliance with this policy.

Unacceptable Use by Staff

All employees should use their own judgment regarding what is unacceptable use of the school's systems. The activities below are provided as examples of unacceptable use; however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities are detrimental to the success of the school. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.
- All activities for personal benefit only have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).
- All activities that are inappropriate for the school to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.
- Circumventing the IT security systems and protocols which the school has put in place.

Enforcement

The school will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.

Based on the severity of violation the following steps will be taken

First Violation		
Verbal warning by Section Head / HSE		
Ms. Anni M. Jones	Middle Section Head	sectionheadmid@tallah.habitatschool.org
Ms. Neethu Jomon	Primary Section Head	sectionheadpri@tallah.habitatschool.org
Ms. Sheelu Bajpai	KG Section Head	sectionheadkg@tallah.habitatschool.org
Ms. Anjana Geothendran Pillai	Grade 5–12 Girls Section Head	sectionheadgirls@tallah.habitatschool.org
Mr. Anuraj Geetha Sudhakaran	Grade 5–12 Boys Section Head	sectionheadboys@tallah.habitatschool.org
Verbal warning by Section Head / HSE - Non - Teaching Staff		
Mr. Rinu Regi	HSE Officer	sssupervisor@tallah.habitatschool.org
Second Violation		
Memos will be issued by the Principal for teachers and by the Administrative Officer for non-teaching staff.		
Ms. Mariyam Nizar Ahmed	Principal	principal@tallah.habitatschool.org
Mr. Uvais Valiyaneerilakkal	Admin Officer	ao@tallah.habitatschool.org
Third Violation		
Use of any school resources for any illegal activity will usually be grounds for summary dismissal, and the school will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.		

5. **Use of IT systems / Internet by Students**

This policy is applicable to all students in Habitat School.

- Any IT or electronic devices should be used only after the respective teachers' permission. ·
- All devices should be used in a responsible manner.
- Use electronic resources, including storage space, only for educational purposes related to work in schools, and not for any personal, commercial or illegal purposes.
- Use the Internet only with the permission of the staff member in charge.
- Using web browsers for educational purposes of research and information gathering from various websites and databases.
- Using the internet for sharing documents and assignments promoting collaborative work.
- Keeping the allocated personal username and password confidential, not sharing with Anyone and changing the password in regular intervals.
- Not trying to access and change any other person's username, password, files or data. ·
- If the previous person is not logged out, ensure to either log out and use your credentials, or approach the ICT department for support.
- Sharing emails only with people known to oneself and approved by parents or teachers ·
- Using the internet to do online tests or tasks approved or advised by the teachers ·
- Studying syllabus content online and for doing projects or presentations for the lessons pertaining to it with teachers' authorization.
- Approach your OSL and report any activity which seems unusual or confusing to you or if you are facing any form of bullying.

Unacceptable use of IT systems / Internet for students

- Do not change any device settings without permission from ICT department.
- Do not view prohibited online content. Report it immediately to your Online Safety Leader if you come across any issues.
- Do not share copyrighted materials.
- Do not send, upload, download, or distribute offensive, threatening, obscene or religious materials · Do not share school copyrighted material (school logo, worksheets, question papers, soft copies of any school owned material)
- Do not write or label on school devices.
- Destroying, modifying or misusing devices or software in any way.
- Installing or downloading software or products that might harm the device or the network. ·
- Students should not share passwords to any other user, nor attempt to learn or to use anyone else's password, and do not transmit your address or telephone number, or any personal or confidential information about yourself or others. (except your parents). ·
- Do not use the system if the previous user has not logged out.
- Do not save personal files or data on school systems.
- Do not download or install any program, software or hardware without permission.
- Non-compliance with the positive behavior rules inside the cyber lab.
- Students should not attempt to access, upload, or transmit material that attacks ethnic, religious or racial groups, or material that is pornographic or explicitly sexual in nature.
- Students should not upload, link, or embed an image of yourself or others to unsecured, public sites without teacher's permission and a signed parental permission slip
- Students should not make statements or use the likeness of another person through website postings, email, instant messages, etc., that harass, intimidate, threaten, insult, libel or ridicule students, teachers, administrators or other staff members of the school community, make statements that are falsely attributed to others, or use language that is obscene.

Unacceptable use during Live classes for students

- Private conversation or discourse that are not related to study and hinder the course of the lesson during the live broadcasting of the distance learning period.
- Adding any unauthorized program, including programs that are shared and free programs. · Playing games (except with the express permission of the teacher because it is an educational necessity linked to the lesson).
- Misusing rights and tools available from school
- Engaging in audio and video communication with the rest of the students for non-educational purposes after the end of the official period time, be it on or off school premises. · Removing the teacher or students from the group leads to blocking the course of the lesson, teacher's work and other students' rights.
- Abusing or insulting official visitors during the live broadcast. · Participating in unofficial mailing lists bulletins within the distance education initiative and posting information about teachers and students without permission.
- Divulging other students' personal information, including home addresses and phone numbers. · Destroying, modifying or misusing devices or software in any way.

Enforcement

The school will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, students should be aware that actions will be taken in accordance with the school behavior management policy and Online Safety Policy.

5. Data Security & Data Protection

- All students, employees, and organization data (Habitat Schools Data) is the property of the Habitat School. Users must take all necessary steps to prevent unauthorized access to confidential information. Users are expected to exercise reasonable personal judgment when deciding which information is confidential.

- Users must not send, upload, remove on portable media or otherwise transfer to a non- school system any information that is designated as confidential, or that they should reasonably regard as being confidential to the school, except where explicitly authorized to do so in the performance of their regular duties.
- Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with the school's Password policy.
- Habitat Schools Data is not to be shared with a third party, including parents or community residents, unless authorized to do so in the performance of their regular duties.
- Users who are supplied with computer equipment by the school are responsible for the safety and care of that equipment, and the security of software and data stored on other school systems that they can access remotely using it.
- Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.
- All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.
- Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.
- Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the school's systems by whatever means and must report any actual or suspected malware infection immediately.
- Access to Habitat Schools Data will only be provided after acceptance and signature of the Acceptable Use Policy.

Laws are in place for a reason:

1. Refrain from violating copyright laws, damage or tamper with hardware or software, vandalize or destroy data, intrude upon, alter or destroy the files of another user, introduce or use computer "viruses," attempt to gain access to restricted information or networks, or block, intercept or interfere with any email or electronic communications by teachers and administrators to parents, or others.

2. Also understand that the prohibited conduct described above is also prohibited off campus when using private equipment if it has the effect of seriously interfering with the educational process, and that such off-campus violations may lead to disciplinary measures.

3. Students should not imply, directly or indirectly, either publicly or privately that any program or "app" you create is associated with, or a product of, the school, nor will you either directly or indirectly associate any such program with any School logos or images, unless it is required and authorized by school authorities.

Know the consequences of plagiarism.

Acceptable use guidelines for Parents

The Acceptable Use Policy is intended to ensure.

- that students will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to read and understand the school policies which are published in the school website and parent portal. The school has also published a Fair Processing Notice on the School website which explains how the school handles personal information.

Parents are requested to sign the agreement form below to show their support of the school in this important aspect of the school's work.

Acceptable Use Agreement for Kindergarten students

This form relates to the *student/pupil* Acceptable Use Agreement.

Please complete the sections below to show that you have read, understood and agreed to the rules included in the Acceptable Use Agreement. Where required, a parent/carer can explain the rules to young children.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers.
- Only engage in activities that a teacher or suitable adult has told or allowed me.
- Take care of computers and other equipment.
- Never send a picture of myself and others to anyone without parents' permission.
- Not communicating with strangers online.
- Ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- Tell a teacher or suitable adult if I see something that upsets me on the screen ·
- Follow all internet rules set by my parents and teachers.

I have read and talked about these rules with my parents/guardian.

Name of Student: .....

Class & Division: .....

Signature: .....

Date: .....

Parent/Carer Name and signature: .....

Acceptable Use Agreement for Younger Age students
(Grade 1 - Grade 5)

This form relates to the *student/pupil* Acceptable Use Agreement.

Please complete the sections below to show that you have read, understood and agreed to the rules included in the Acceptable Use Agreement. Where required, a parent/carer can explain the rules to young children.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers.
- Only engage in activities that a teacher or suitable adult has told or allowed me. · Take care of computers and other equipment.
- Never send or post personal information, such as my address, phone number, password, school name of myself and others.
- Never send a picture of myself and others to anyone without parents' permission.
- Not open emails from unknown people.
- Not communicating with strangers online.
- Not follow links to websites that I don't recognize.
- Only send messages online which are polite and friendly.
- ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- Tell a teacher or suitable adult if I see something that upsets me on the screen · Follow all internet rules set by my parents and teachers.
- I know that if I break the rules I might not be allowed to use a computer.

I have read and talked about these rules with my parents/guardian.

Name of Student: .....

Class & Division: .....

Signature: .....

Date: .....

Parent/Carer Name and signature: .....

Acceptable Use Agreement for Older Age students

(Grade 6 - Grade 12)

This form relates to the *student/pupil* Acceptable Use Agreement.

Please complete the sections below to show that you have read, understood and agreed to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

For my own personal safety

- I understand that the school will monitor my use of the systems, devices and digital communications. ·
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online. I will try to contact the school social worker/Online safety leader if I feel discomfort online.
- I understand that everyone has equal rights to use technology as a resource. ·
- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission. ·
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work. ·
- I understand that it may be a criminal offence or breach of the school policy if I download or share inappropriate pictures, videos, or other material online.
- I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18.
- I will not use the *school* systems or devices for online gaming, online gambling, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

- *I will act as I expect others to act toward me,*
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others,
- I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. ·
- I will not take or distribute images of anyone without their permission.
- *I recognize that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school.*
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organization who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research/assignment or recreation, I recognize that,

- Should ensure that I have permission to use the original work of others in my own work · Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- *I understand that I am responsible for my actions, both in and out of school,*
- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, which are covered in this agreement, when I am out of school and where they involve my membership of the school community.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action.
- *I have read and understand the above and agree to follow these guidelines when:*
- I use the school systems and devices (both in and out of school)
- I have read and talked about these rules with my parents/carers.

I have read, understood and agreed to comply with the School Acceptable Use of Policy.

Name of Student: ……...

Class & Division: .....

Signature: .....

Date: .....

Signature of Parent: ……

Acceptable Use Agreement for Parents

Parents are requested to read and understand the school policies which are published in the school website and parent portal. School has also published a Fair Processing Notice on the School website which explains how the school handles the personal information.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use agreement is attached to this form, so that parents/carers will be aware of the school expectations of the young people in their care.

The Acceptable Use agreement is intended to ensure,

- · That student will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use. ·
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- · That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

Parents are requested to sign the agreement form below to show their support of the school in this important aspect of the school's work.

Agreement Form

Parent/Care

Name: .....

Student Name: .....

Grade and Division: …….

As the parent/carer of the above student, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

As a parent/carer, I have received an Acceptable Use Agreement for my ward and have briefed the same to him/her and understand that he /she will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

I have read, understood and agreed to comply with the School Acceptable Use agreements.

Signature: .....

Date: .....

Contact

If you have any queries or concern regarding this policy, then please contact itsupport@tallah.habitatschool.org.