

Reference number	A8	Policy name	Whole School Digital Technology Policy
------------------	----	-------------	----------------------------------------

Person responsible	JWE	Date of next review	November 2024
Policy links	C1, C4. D1, D5. E1, E2, E6, E10, F4, I1, I2 (Also B1, B3, D3, J1)		

Vision, mission and values	To promote safe and acceptable use of digital platforms, educational resources, and whole school digital infrastructure.
Rationale	<p>Excellence in education requires that technology is seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future to enable students to maximise their full potential and to prepare them for college and the workplace. Learning results will improve from the continuous dynamic interaction among students, educators, parents, and the extended community. Technology immersion does not diminish the vital role of the teacher. To the contrary, it transforms the teacher from a director of learning to a facilitator of learning.</p> <p>The internet and associated technologies are powerful tools for learning. They have the potential to access information at high speed and to empower children to take an increased level of ownership over their learning. The use of the internet and associated technologies in school are tools that provide our children with exciting opportunities to pursue 'personalised learning'. The purpose of this policy is to clearly identify guidance and best practice pertaining to all elements of Uptown International School's digital platforms, ensuring that all online safety risks are minimised, not only for children and young people, but for their parents and the other members of the school community.</p> <p>This is managed through 3 key areas:</p> <ul style="list-style-type: none"> ▪ Leadership and Policy ▪ Infrastructure ▪ Education

WSLT sign off		Date	November 2023
---------------	-------------------------------------------------------------------------------------	------	---------------

TABLE OF CONTENTS

LEADERSHIP AND POLICY	5
Online Safety Group	5
INFRASTRUCTURE.....	6
Password Policy	6
Password and authentication protocols, monitoring and reporting:.....	6
Authentication	7
Reporting a Suspected Compromise or Breach	8
Filtering	8
Technical Security Strategy	8
Data Collection.....	9
Purpose	9
What is Personal Information?	9
Data Protection Principles:	9
General Statement:	10
Systems/processes/storage/monitoring responsibilities:	10
EDUCATION	10
Staff.....	10
Children and Young People.....	11
Digital Citizens	11
User expectations	11
Consequences of violations	12
Appeals process	12
DIGITAL PLATFORMS	12
Primary.....	12
Staff:.....	12
Students:	13
Secondary	14
Summary	14
Staff:.....	15
Students:	16

ARTIFICIAL INTELLIGENCE.....	16
Responsible Use of AI	16
Guidelines for Students	17
Guidelines for Teachers and Staff.....	17
Parents and The Wider Community	18
E-Safety at Home	18
APPENDICES	19
UIS STAFF ACCEPTABLE USE POLICY – APPENDIX 1	19
Penalties:	21
Staff access to email, social networks and the internet:	21
Email and instant messaging:.....	21
Social networks:.....	22
Unfiltered internet access:	22
Home access:	22
Penalties:	23
UIS SOCIAL MEDIA POLICY FOR STAFF – APPENDIX 2	24
Implementation of the policy:	24
Relationship with other school policies:.....	25
Responsible use of social media	25
Personal use of social media.....	26
The monitoring of social media.....	27
Social media and the end of employment	28
UIS SOCIAL MEDIA POLICY FOR STUDENTS AND PARENTS – APPENDIX 3.....	28
Personal Use of Social Media:.....	29
Using Social Media	30
Monitoring of Internet Use.....	30
Breaches of this Policy.....	30
TAALEEM ACCEPTABLE USE POLICY/BRING YOUR OWN DEVICE POLICY – APPENDIX 4	31
The Rationale:.....	31
BYOD includes all Mobile devices and any wearable technology	31
Social Media	31
Taking Care of school mobile devices.....	32
General Precautions	33

Carrying Mobile devices	33
Screen Care	33
Using Mobile and BYOD devices at School	34
Screensavers/Background photos/Apps	34
Sound, Music, Games, or Programs.....	34
Printing.....	34
Saving to the Mobile device/Home Directory	34
Network Connectivity.....	35
Originally Installed Software	35
Additional Software	35
Inspection	35
Procedure for re-loading software	35
Software upgrades	35
Acceptable Use	36
Parent/Guardian Responsibilities	36
School Responsibilities are to:	36
Students are Responsible for:	36
Student Activities Strictly Prohibited:	37
Mobile device and BYOD Care	38
Mobile device theft	38
Legal Propriety	38
Protecting & storing of the Mobile and BYOD devices	39
AUP/BYOD User Pledge	39
The following applies for BYOD devices	40

LEADERSHIP AND POLICY

Online Safety Group

Uptown International School (UIS) has a designated Online Safety Group who oversee policy and practice relating to all elements of online safety and digital platforms:

- **Principal:** To take overall responsibility for the safety and security of online systems and digital platforms and to make final decisions pertaining to policy and practice.
- **Head of Secondary:** To take overall responsibility for the implementation and monitoring of educational technology, and to oversee breaches of policy across the Secondary school.
- **Head of Primary:** To take overall responsibility for the implementation and monitoring of educational technology, and to oversee breaches of policy across the Primary school.
- **UIS IT Support:** To oversee Whole School Digital Infrastructure and associated policies.
- **Assistant Head of Secondary and Designated Safeguard Lead:** To oversee all elements pertaining to Digital Safeguarding in the Secondary School.
- **Assistant Head of Primary and Designated Safeguard Lead:** To oversee all elements pertaining to Digital Safeguarding in the Primary School.
- **Assistant Head of Secondary – Digital Platforms:** To take overall responsibility for Digital Platforms within the Secondary School
- **Assistant Head of Primary – Digital Platforms:** To take overall responsibility for Digital Platforms within the Primary School

All members of the school community are expected to take responsibility for using technology positively. As well as training, the following is in place:

- All staff are expected to sign to confirm they have read and understood the Acceptable Use Policy.
- All staff are expected to sign to confirm they have read and understood the Staff Handbook.
- All children are expected to have been taken through and understood the AUP/BYOD Policy.

The Online Safety Group are responsible for reviewing and amending the following school policies on an annual basis:

- UIS Staff Acceptable Use Policy – Appendix 1
- UIS Social Media Policy for Staff – Appendix 2
- UIS Social Media Policy for Students and Parents – Appendix 3
- UIS Cyber Bullying Policy – Refer to Policy E10 (Anti Bullying Policy)
- Taaleem Acceptable Use/BYOD Policy – Appendix 4

INFRASTRUCTURE

Password Policy

Password and authentication protocols, monitoring and reporting:

All users are responsible for their login and password credentials. Passwords must meet the complexity requirements and must not be shared with anyone. User logins and passwords are one of the primary protections employed to restrict access to the school network and school online platforms including Microsoft Office apps. If a password is compromised, access to systems can be obtained by an unauthorised individual.

Users with logins are responsible for safeguarding against unauthorised access to their account, and as such, must ensure passwords are kept confidential. All passwords should be designed to be complex and difficult to breach, using AD and Microsoft logins to use in our systems.

Below are the systems or portals that can be logged in:

- School computers – for both staff and students,
- UTS –BYOD WIFI network – for both staff and students,
- UTS-WIFI Network – For school owned devices (staff laptops, school iPads),
- UTS-GUEST WIFI Network -Guest users visiting school,
- UTS-EVENTS WIFI Network – For school events or training,
- ISAMS – staff,
- CPOMS – staff,
- Office 365 – staff and students,
- Proactive – staff,
- IT Service desk – staff,
- Toddle – for both staff, students, and parents,

Users can change their password directly from a school owned computer if they know their current password.

In Windows: Press ctrl + Alt + Delete > select change password.

In iMac: From System preference > users and groups > change password.

If any user forgets their password, they must contact IT support and request a password reset. Students requiring a password reset can contact IT after informing the classroom teacher.

All users and system passwords should meet the following characteristics:

- Be at least 8 characters in length,
- Consist of a mix of alpha, and at least one numeric, and special symbols,
- Not be portions of associated account names (e.g., user ID, log-in name),
- Not be character strings (e.g., ABC or 123),
- Not be simple keyboard patterns.

Passwords must be changed at least every 42 days. Previously used passwords cannot be re-used.

Authentication

Secondary students: if a secondary student forgets a password, he\ she can contact IT support after informing the teacher. Password reset email requests from students will be ignored and replied with the message 'forward through homeroom teacher'.

Primary students: To avoid forgetting passwords and to alleviate the need to reset passwords in the current situation, primary students are automatically set with a unique complex password. It can be changed from the students' side but may not expire after 42 days. This setting can be changed if there is a request from educational heads.

Staff: Staff can submit a request IT support for a password reset from their personal emails. However, the new IT provided password should change after signing in.

Staff logins are secured with multi-factor authentication from Microsoft (MFA). All the staffs' personal devices are registered in Microsoft cloud. The user needs to authenticate their device for a successful login to email and online portals. System fails to sign in will occur in the absence of successful authentication.

Reporting a Suspected Compromise or Breach

If you believe your password has been compromised or if you have been asked to provide your password to another individual, immediately change your password and promptly notify IT support teams.

[https://servicedesk.taaleem.ae/
itsupport@uptownschool.ae](https://servicedesk.taaleem.ae/itsupport@uptownschool.ae)

FAO: Ubyis or Marites.

042515001 ext: 205 or 232

If you suspect you have received a phishing email, please forward it immediately to itss@taaleem.ae and each reported instance will be investigated from IT department.

Filtering

Explicit guidance and information pertaining to UIS and how we monitor/log/update.

System filtering at UIS is overseen by Taaleem Central Office IT Department, however it is at the discretion of UIS as to what should be filtered\blocked or unblocked. Requests to block, monitor or update will be forwarded to Taaleem Central Office IT Department. UIS IT support will then act accordingly. Websites falling under virus, malicious, inappropriate content areas are blocked with the help of Fortinet firewall.

Social media websites are blocked in students BYOD and UTS-GUEST WIFI networks.

Technical Security Strategy

System backups/network resilience/protocols for external breach of security

- UIS system backups are the responsibility of Taaleem Central Office IT Department,
- All UIS devices on campus are authenticated with Mac ID \Microsoft \ AD login using UCOPIA controller,
- Devices without preregistration or user login will not be allowed access to campus Wi-Fi and other portals,
- **Anti-Virus:** ESET Anti-virus software to be installed on all the school computers,
- **Updates:** periodic updates will be installed centrally over our servers\ networking devices or physically by the IT staff in school owned computers and laptops,
- Personal devices – Staff, Students and Guest users are expected to follow wise use of school Internet and technology. To ensure the security and threat protection, all users are required to have anti-virus software installed on their personal devices. Users should not use personal devices in school if it is affected by any virus, malware or any similar threat applications and programs,

- personal devices logs or network traffic logs may monitor as part of any investigation to determine proper use,
- No staff may knowingly disable any network software, antivirus or any system identified as a pre-installed monitoring tool.

Data Collection

UIS 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 it 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.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with international best practice. 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.

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.

Data Protection Principles:

The following principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary, kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects in line with international best practice.
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security.

General Statement:

The school is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected,
- Inform individuals when their information is shared, and why and with whom it was shared,
- Check the quality and the accuracy of the information it holds,
- Ensure that information is not retained for longer than is necessary,
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely,
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded,
- Share information with others only when it is legally appropriate to do so,
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests,
- Ensure our staff are aware of and understand our policies and procedures.

Systems/processes/storage/monitoring responsibilities:

- Students and staff primary data: ISAMS - managed by the Data Manager,
- Students and staffs' homework and reports: iSAMS, Toddle and Seesaw - managed by the Data Manager,
- Email and Work-related documents – Students, staff emails and work-related data stored in cloud with Microsoft. Access to this is controlled by the username and passwords, also multi factor authentication for the staff data – managed by IT support,
- Microsoft accounts and App data - managed by Taaleem central office IT team and school IT support.

EDUCATION

Staff

UIS is committed to ensuring all members of our extended community are kept abreast of the latest developments in technology, by providing appropriate educational resources for students, parents, and staff alike.

We are a certified National Online Safety School and as such have access to an extensive range of education resources and designated school and parental portals to provide our community with relevant information and guidance. Examples include:

- Digital platform guides,
- Educational video content,
- Webinars,
- Training and CPD.

Safeguarding and promoting the welfare of children is everyone's responsibility. All staff have a responsibility to provide a safe environment in which children can learn. This includes protecting children from online harm and abuse, and risks such as CSE, online bullying or online sexual harassment. School staff should receive online safety training that is integrated, aligned, and considered as part of the overarching safeguarding approach.

Children and Young People

UIS is committed to ensuring its students are well informed and well skilled in the advantages and disadvantages of working in a digital age. Key, age specific skills are taught throughout the curriculum to ensure students have the necessary tools to engage with technology successfully. Students, through carefully crafted curriculum opportunities are also taught of the importance of online safety, their digital footprint and how to navigate digital platforms.

UIS is a certified National Online Safety school and uses its extensive resource bank and up to date information to educate students on all aspects pertaining to digital safety and usage.

Digital Citizens

UIS is dedicated to ensuring that students become responsible digital citizens through ethical engagement with the digital world. A commitment to providing a safe inclusive online environment, where students are respectful of others, and individual rights are protected is a priority.

User expectations

As users of the UIS digital platforms, students will be expected to:

- Respect Others
 - Treat all individuals with respect and dignity.
 - Avoid engaging in or promoting hate speech, harassment, discrimination, or cyberbullying.
- Protect Privacy
 - Not share or misuse personal information about themselves or others.
 - Respect and adhere to UIS privacy policies and guidelines regarding data collection and sharing.
- Uphold Intellectual Property Rights
 - Not share or distribute copyrighted material without authorization.

- Ensure that any content posted is either original or attributed to the original source.
- **Maintain Security**
 - Safeguard accounts and personal information using strong, unique passwords.
 - Report any security breaches to administrators promptly.
- **Foster Positive Interactions**
 - Engage in constructive and meaningful digital conversations.
 - Encourage positive and respectful communication with other users.
- **Follow Platform Guidelines**
 - Adhere to respective platform's terms of service.
 - Comply with specific content or conduct policies related to the terms and services and features offered by the Respective Platform.
- **Report Violations**
 - Report any violations of digital citizenship guidelines.

Consequences of violations

- Failure to comply with the UIS digital citizenship principles may result in but not exhaustive:
 - Warnings and notifications regarding inappropriate conduct.
 - Temporary suspension of accounts.
 - Legal actions in cases of criminal activity or breaches of law.

Appeals process

Should it be believed that a decision related to a violation of these digital citizenship guidelines is unfair, appeals may be launched through school managers and administration.

DIGITAL PLATFORMS

Primary








Staff:





- Seesaw – Staff view and set student work on this digital portfolio. Staff have the ability to share work and learning with both parents and students. They are also able to communicate with the parents and the students.
- My Maths – Teachers provide mathematics home learning through this platform. Students login to complete their assigned activities.
- TT Rockstars – Teachers facilitate the learning of Timetables through this platform.
- Bug Club – teachers use this platform to allocate e-readers to students.
- Lexonik – used to support students' literacy skills.
- Toddle – an IB specific learning and assessment platform for students and teachers.

Students:

- Seesaw – Online digital portfolio. Students access activities and upload activities completed in school and home. Students are also able to share experiences with school and their family through the application. Students can be permitted to view the learning of other children.
- MyMaths – Students access mathematics learning that has been set by the teacher.
- TT Rockstars – A platform that provides students with the opportunity to develop their timetables understanding.
- Epic Reading – Students are provided with e-readers that are read to them from this website.
- Bug Club – Students are provided with e-readers from this platform.
- Lexonik – used to support students’ literacy skills.
- Toddle – an IB specific learning and assessment platform for students and teachers.

Secondary Summary

Whole School Platforms	ISAMS 	https://uts.isams.cloud/	IT Support	Whole school student information system & school management.
	CPOMS 	Login - CPOMS	MWR	Logging behaviour and safeguarding
	Toddle 	DP Home (toddleapp.com)	CDA/ADU	Whole school platform for curriculum management; student calendars; assignments; unit plans; informal communications.
	Microsoft Teams 	Launch Application	IT Support	Used for Teams calls/meetings only. No longer used for any assignments.
	OneNote 	Launch Application	IT Support	Used for organising and distributing packs of digital resources. UIS Professional Learning Notebook
	Microsoft SharePoint 	Secondary Staff SharePoint	IT Support	Online folder structures for shared groups. E.g. UIS Diploma Programme
	Microsoft One Drive 	Individual Account	IT Support	Online cloud storage.

	Turnitin 	Integrated with Toddle	ADU	Plagiarism detection software that is integrated with Toddle.
Subject Specific Platforms	Kognity 	Teacher Home Kognity	ADU	Digital textbook. Teacher have the ability to set and track reading/question assignments.
	InThinking 	ThinkIB	HOD	Popular DP resource and activity bank.
	QuestionBank 	IB Questionbank (ibo.org)	HOD	Official IBO exam creation software using previous exam questions.

Staff:

Staff have access to the following digital platforms:

- CPOMS – This is the central platform staff use to log all incidents about a child, including those of a sensitive nature as per our child protection policy.
- ISams – The school’s Management Information System, where all formal records of students are stored and where registers are taken.
- Lexonik – used to support students’ literacy skills.
- Toddle– used as a platform for monitoring planning and assessment, along with IB specific elements such as personal project, SA and CAS and for report writing.
- Microsoft Office
- Office – Staff have access to Microsoft Office online, allowing them to compose work in different office formats.
- Outlook – Designated staff email account.
- Teams – Main platform for video conferencing external and internal.
- One Note - Is used to share all teaching and learning resources with students, and as a platform to set and submit work or have students work collaboratively in groups.
- OneDrive – Personalized cloud-based storage.

- Share Point – School wide cloud storage.

Students:

In the Secondary School, students utilize the full functionality of Microsoft 365 as follows:

- Outlook – Designated school authorised and regulated email account.
- Teams – Used for online meetings and video communication internally and externally.
- One Note - Class Notebook is used to access all teaching and learning resources with students, and as a platform to submit work or work collaboratively in groups.
- OneDrive – Personalized cloud-based storage.
- Office – Students have access to Microsoft Office online, allowing them to compose work in different office formats.
- TT Rockstars – A platform that provides students with the opportunity to develop their timetables understanding.
- Lexonik – used to support students’ literacy skills.
- Toddle – an IB specific learning and assessment platform for students and teachers.

ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is a rapidly evolving technology with the potential to revolutionise various aspects of our lives, including education. This policy outlines the guidelines for the acceptable use of AI within our school community, ensuring that it benefits both students and staff while maintaining safety, privacy, and equity.

With regards to AI, UIS is committed to:

- Promoting responsible and ethical use of AI technology within the school environment.
- Ensuring that the integration of AI enhances the educational experience and does not compromise privacy or security.
- Encouraging innovation and creativity in leveraging AI for educational purposes.
- Establishing clear expectations for students, teachers, and staff regarding the use of AI.

Definitions

- **AI Technology:** Any software or hardware system that employs machine learning, data analysis, or automation to perform tasks or make decisions without explicit programming.

Responsible Use of AI

Educational Enhancement

AI may be used to enhance educational experiences, such as personalised learning, data analytics for performance improvement, and educational software. The primary goal is to improve learning outcomes and promote academic success.

Privacy and Data Security

- Staff must not share personal data of students with any AI systems. All data collected or generated by AI systems must be stored securely and used solely for educational purposes.
- Personally identifiable information (PII) must be protected according to relevant laws and regulations, such as the Family Educational Rights and Privacy Act (FERPA).
- Consent must be obtained from students and parents/guardians before collecting any personal data for AI-driven educational purposes.

Ethical Considerations

- AI systems must not perpetuate bias or discrimination. Efforts should be made to ensure fairness and equity in their design and use.
- Teachers and students should be educated about the ethical implications of AI technology and encouraged to discuss these issues in the classroom.
- Any use of AI that may infringe upon the dignity or privacy of individuals should be avoided.

Guidelines for Students**Responsible Use**

- First and foremost, it's essential for students to actively engage with AI as a supplement to their learning, not a substitute. AI can aid in research, data analysis, grammar and spell-checking, and even generating suggestions for improvement. However, it should never replace the critical thinking, creativity, and problem-solving skills that are the core objectives of education.
- Students must also be aware of the ethical considerations surrounding AI usage. This includes citing AI-generated content appropriately, ensuring data privacy and security, and avoiding plagiarism by properly attributing AI-generated assistance in their work.
- Furthermore, students should use AI as a learning opportunity. They should actively seek to understand the algorithms and processes behind AI tools, allowing them to make informed decisions about when and how to utilize AI in their academic pursuits.
- Students are expected to use AI technology responsibly, following the school's code of conduct and adhering to this policy.
- Misuse of AI technology for cheating or academic dishonesty will not be tolerated. See updated academic honesty policy.

Reporting Concerns

- Students should report any concerns regarding the use of AI technology that may violate this policy to a teacher or school administrator.

Guidelines for Teachers and Staff**Integration into Curriculum**

- Teachers are encouraged to integrate AI technology into their curriculum when appropriate and beneficial for student learning.
- Training and professional development opportunities will be provided to help teachers effectively use AI in the classroom.

Monitoring and Accountability

- Teachers and staff members using AI systems are responsible for ensuring that they are used in compliance with this policy and applicable laws.
- They should report any technical issues or ethical concerns related to AI technology.

Compliance and Enforcement

Violations of this policy may result in disciplinary action, including but not limited to warnings, loss of access to AI technology, or other appropriate consequences. Decisions will be made on a case-by-case basis.

Review and Revision

This policy will be reviewed periodically to ensure its effectiveness and relevance in the ever-changing landscape of AI technology. Any necessary revisions will be made to reflect new developments and best practices.

Parents and The Wider Community

A designated online parent portal in our National Online Safety platform allows parents the opportunity to access a wide range of resources, webinars and courses to enable them to proactively educate themselves around topics associated with digital safety.

E-Safety at Home

In addition to our NOS platform, there are several sites that offer helpful advice to parents/carers, particularly with respect to how they can best monitor their child's use of the computer at home. Here are some parents/carers might like to try:

- <https://esafe.ae/>
- www.saferinternet.org.uk
- www.childnet.com
- www.anti-bullyingalliance.org.uk
- www.nspcc.org.uk
- <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security>

The following useful publications are also of use:

- [DfE Advice for Parents on Cyberbullying](#)
- [Childnet Cyberbullying Leaflet](#)
- [DfE The use of social media for on-line radicalisation](#)
- [UK Council for Child Internet Safety](#)
- [Alert to students: The legal dangers of sexting](#)

APPENDICES

UIS STAFF ACCEPTABLE USE POLICY – APPENDIX 1

The use of technology at UIS is extended to staff who wish to enhance their teaching and administrative functions. Those working within the proper guidelines as outlined in this policy will receive the maximum benefits of the computer network. In order to facilitate effective working practice and advance the use of such technology, each user may make use of all authorised hardware and software in the school. Each user may also use available and authorised email and internet access in order to retrieve information from a variety of educational resources.

Responsibilities regarding hardware, software and the school network:

- The user exercising his/her right to use any hardware or software as an educational resource shall also accept the responsibility for its preservation in a good condition,
- Only those users who have received induction training shall be authorised to use any of the hardware or software. A briefing of new facilities and introduction to this AUP is held for new staff during induction at the start of each new academic year, any existing staff who need refresher information should attend this briefing or arrange with IT Support for such training to be delivered as soon as the need is identified,
- Make sure no hardware or software is destroyed, modified or abused in any way,
- Keep programs and files of a viral, illegal, or damaging nature off the school's equipment,
- Obtain permission from IT Support prior to removing, relocating, disposing of, or modifying any hardware or software,
- Ensure that food or drink is not allowed near any computer or any other electronic equipment,
- Report any unauthorised use of the user's account directly to IT support or Senior Leader,
- Ensure that insurance is in place to indemnify the user if the computer is taken out of the UAE or left unattended in a place where theft or loss is not covered by the school's insurance policies.

The following is a list of prohibited activities. This is not exhaustive and is subject to review.

Staff:

- Shall not use any other school account other than the school account assigned to them nor allow non-UIS personnel or other users to use their school laptop or access the school data services or networks,
- Shall not attempt to bypass accounting or security mechanisms, or to investigate files, programs, or directories outside the areas assigned to them. They will not attempt to exit from the username allocated to them by IT Support nor seek to modify or subvert the network or laptop/workstation operating system,
- Shall not attempt to sabotage the school networks in any way, i.e. corrupting files, transferring viruses, damaging the file system, deleting files other than their own, etc.,
- Shall not modify, vandalise, or neglect the computer equipment or components,
- Shall not use, copy, or disseminate text, graphic or program files of an inappropriate, obscene, or pornographic nature or attempt to circumvent copyrighted materials by use of software tools for downloading or distributing such materials. This includes torrent or other file-sharing software,
- Shall make every effort to avoid websites and other resources that may introduce malware onto the school computers or network,
- Shall not install software that contravenes any part of this AUP or is in any way contrary to copyright and intellectual property rights,
- Shall not divulge passwords or other credentials nor leave themselves logged on to their account when they are not present in the room and should immediately change default passwords to individual secure ones. Advice on this can be sought from IT Support,
- Staff should be aware of the potential dangers of using smartphones and tablet computers to access school data systems across public Wi-Fi, when transiting Wi-Fi zones and when using 3G/4G/5G especially if the phone is unlocked and/or has security features disabled,
- Staff are asked to refrain from using school data systems on such devices unless suitable security measures are applied.

The school, by means of designated personnel, retains the right to monitor, view and maintain all aspects of the computer systems and network including individual storage of files. Files containing inappropriate, obscene, or pornographic material or file names may be deleted and/or copied for evidence without warning by IT Support or if subject to an access request by an authorised body. Dangerous, unnecessary time-wasting or reckless behaviour online may also be reported.

Penalties:

The guidelines outlined in this policy are not all inclusive nor exhaustive; other violations not specified but similar in outcome will be dealt with accordingly. Any violations to this policy will have appropriate measures brought to the violator. Any user not conforming to this policy may have intervention strategies and/or disciplinary actions taken by the management and such violation may in extreme cases be deemed as misconduct or gross misconduct as determined by other school policies.

Staff access to email, social networks and the internet:

A filtering system is used by the school that will block access to most of the inappropriate material on the Internet. While quite comprehensive and broadly in accordance with approved specifications, there is no guarantee that staff or students will not encounter objectionable sites. If such materials are encountered staff should alert IT Support who will block them subject to investigation. Electronic information research skills are now fundamental to preparation of citizens and future employees.

School laptop hard drives or SSDs are school property and as such are subject to manipulation and review by designated school officials to maintain system integrity and ensure that users are using the system responsibly. Users should therefore not expect that files on school laptops will always be private. However, the school endeavours to keep email and files private through access permissions and encryption. All email communications may be archived for compliance with data management legislation and safeguarding of content. Staff access and use is not normally monitored other than as a function of normal operating system maintenance, resource allocation and process logs unless so required to do so by a request from the Principal or by a law enforcement agency under the relevant legislation. In which case IT Support will coordinate the school's response.

Email and instant messaging:

Staff are reminded that email sent from the school email systems is linked to a school-owned domain name and as such all communications represent the school. Staff should note that email, social network traffic and instant messaging using school equipment should only be used for bona fide school business. Personal email should therefore be sent through each member of staff's own mail server rather than the school email account.

Social networks:

Staff are required to use social networks responsibly and to consider the ramifications of posting messages from school premises and computers or to online groups with memberships of current students or parents. Where possible and as a default a separate social network from the member of staff's personal account and identity should be used for school purposes. Students should not be exposed to contact with other non-UIS adults across school related social networks nor with staff using their personal email or social network accounts. Pictures of staff and students published on the web should be in line with the school's policy on use of pupil images and staff should be mindful of misinterpretation or manipulation of such images when placed on the world wide web. More detailed guidance can be found in our Social Media Policy.

Unfiltered internet access:

Unfiltered Internet access may be requested when resources that may be required for teaching/research purposes are required. This request will be granted for limited periods and reviewed at the end of that period. Staff laptops will have unfiltered internet access available and therefore care should be exercised when displaying pages from the internet to students. Staff use of the internet may however be automatically recorded by the school's firewall systems. These are reviewed by the Online Safety Group from time to time.

Home access:

Staff using school computers for home internet access remain subject to this AUP. If they require private, unfiltered/unregulated access to the internet they should purchase an internet access package at their own cost. In doing so they are accepting responsibility for their actions and the liability for any occurrence.

The following are not permitted:

- Sending or displaying offensive messages or pictures,
- Gambling,
- Using obscene language,
- Harassing, insulting, or attacking others,
- Damaging computers, computer systems or computer networks,
- Violating copyright laws,
- Using another's password,
- Trespassing in another's folders, work, or files,
- Intentionally wasting resources,
- Employing the network for commercial purposes or making significant financial transactions online,
- Requesting unnecessary and lengthy material that ties up system resources.

Penalties:

Loss or restriction of access.

Additional disciplinary action pursuant to existing practice regarding misconduct up to and including law enforcement agency involvement.

Declaration to be signed by every member of staff with access to the school networks and computer systems:

I agree to abide by the Uptown International School Staff Acceptable Use Policy

Print Name:

Sign Name:

Role:.....

Date:

Signed (for the school).....

UIS SOCIAL MEDIA POLICY FOR STAFF – APPENDIX 2

This policy applies to all members of staff within the school community.

A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chatrooms, media posting sites, blogs and any other social space online. It includes but is not limited to, sites such as Facebook, Twitter, Instagram, Snapchat, TikTok, LinkedIn etc.

This policy applies to the use of social media for both business and personal purposes, whether during school/working hours or otherwise. The policy applies regardless of whether the social media is accessed using the school's IT or network facilities and equipment or using equipment or other resources belonging to the individual concerned or other members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether the school equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with an investigation, which may involve handing over relevant passwords and login details so far as this is consistent with the right of an individual to private and family life.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Implementation of the policy:

The Principal has overall responsibility for the effective operation of this policy but has delegated day to day responsibility for its operation to the UIS Online Safety Group. Responsibility for monitoring and reviewing the operation of this policy and any change to minimise risk to the school also lies with the Principal.

All staff with line management responsibility have a specific obligation for operating within the boundaries of this policy, ensuring that all staff within their remit understand the standards of behaviour expected of them and if necessary, enforcing this policy by taking action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to Heads of School or the Principal. Questions regarding the content or application of this policy may be directed to any member of the Online Safety Group.

Relationship with other school policies:

If an internet post would breach any of our policies in another forum it will also breach them in an online forum. For example, staff may not use social media to:

- breach our obligations with respect to the rules of relevant regulatory bodies,
- breach any obligations they may have relating to confidentiality,
- breach the school's disciplinary rules,
- defame or disparage the school or its affiliates, parents, staff, students, business partners, suppliers, vendors or other stakeholders,
- harass or bully other staff in any way,
- unlawfully discriminate against other staff or third parties or breach the school's Equal Opportunities policy,
- breach the school's Data Protection policy,
- breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Behaviour online can be permanent and so staff must be very cautious about what they say as it may be all but impossible to retract.

Staff must also be aware of the risks to internet security that social media presents. In order to comply with the existing school policy on internet security staff must take any extra measures necessary and not allow any of their actions on social media sites to create any security risk on school equipment or systems.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of their employment.

Responsible use of social media

Staff must be aware that their role comes with particular responsibilities, and they must adhere to the school's strict approach to social media. Staff may be required to use their personal devices to document school events and share with the Marketing and Communications Executive. **If a staff member uses their personal device to take photographs of UIS students or staff. These must be shared only with the Marketing and Communications Executive and then deleted from their device and cloud storage within 24 hours of the event.**

In addition,

Staff must:

- ensure that wherever possible their privacy settings on social media sites are set to private so that students cannot access information relating to their personal lives,
- fully consider the possible impact of any personal profile which they intend to create where the school is named or mentioned on a social networking site and ensure that in so doing they comply with this policy,
- fully consider the possible impact before they write about or make any comments on behalf of the school on the internet or through any social networking site,
- report immediately to the Marketing and Communications Executive or any member of the Online Safety Group if they see any information on the internet or on social networking sites that disparages or reflects poorly on the school,
- immediately remove any internet postings which are deemed by the school to constitute a breach of this or any other school policy,
- weigh whether a particular posting puts their effectiveness as a teacher or member of staff at risk,
- post only what they want the world to see.

Staff must not:

- provide references for other individuals on social or professional networking sites; such references whether positive or negative can be attributed to the school and create legal liability for both the author of the reference and the school,
- use language which might (in the context of the UAE) be deemed to be defamatory, obscene, proprietary, or libelous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations,
- discuss students or colleagues or publicly criticise the school or staff,
- post images on their personal social media sites that include students,
- initiate friendships with students on any personal social network sites,
- accept students as friends on any such sites; staff must decline any pupil-initiated friend requests.

Personal use of social media

The school recognises that staff give good service to the school, and occasionally may want to use social media for personal activities at the office or by means of its computers, networks and other IT resources and communications systems.

The school authorises such use so long as it does not involve unprofessional or inappropriate content and does not interfere with an employee's responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious, or political solicitations, or promotion of outside organisations unrelated to the organisation's business are also prohibited.

Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt or affect the school's IT systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.

Staff should avoid using their work email address for any personal use of social media.

The monitoring of social media

The school's IT resources, and communications systems are the property of the school. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on its electronic information and communications systems.

The school reserves the right to monitor, intercept and review, without further notice, staff activities using its IT resources and communications systems (including but not limited to social media postings and activities) to ensure that its rules are being complied with and the systems are being used for legitimate business purposes. Staff consent to such monitoring by their use of such resources and systems under the terms of the staff Acceptable Use Policy. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The school may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

If a member of staff has any matter that they wish to be kept private or confidential from the school, they should not use its IT resources and communications systems.

Social media and the end of employment

If a member of staff's employment with the school should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that he or she is no longer employed or associated with the school.

All professional contacts that a member of staff has made through their course of employment with the school belong to the school, regardless of whether the member of staff has made social media connections with them or not.

UIS SOCIAL MEDIA POLICY FOR STUDENTS AND PARENTS – APPENDIX 3

The internet provides a range of social media tools that allow users to engage and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly.

While recognising the benefits of a range of social media applications as a popular medium of communication, it is also important to ensure that we balance this with our duties to the school and the community and our legal responsibilities. For example, the use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

This policy sets out a framework of good practice that students, staff and the wider community are expected to follow when using social media in any way that relates to Uptown International School. The principles set out in this policy are designed to ensure that social media is used responsibly and that the confidentiality of students and staff and the reputation of the school are protected.

This policy applies to UIS students, parents and to the wider school community. It covers the personal use of social media as well as the use of sites hosted and maintained on behalf of the school. Under no circumstances may UIS logos, typefaces or brands be used or published on any personal web space or on any online or offline medium without prior consent. These are the property of UIS.

This policy applies to personal web space such as social networking sites (for example *Facebook*, *TikTok*, *Instagram*, *SnapChat*), blogs, microblogs such as *Twitter*, chatrooms, forums, podcasts, *WhatsApp*, open access online encyclopedias such as *Wikipedia*, social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium.

- Users should be conscious at all times of the need to keep their personal and professional lives separate. They should not put themselves in a position where there is a conflict between the school and their personal interests.
- Users should not engage in activities involving social media that might bring UIS into disrepute.
- Users should not represent their personal views as those of UIS on any social medium.
- Users should not discuss personal information on any social media about other parents, students, or school staff.
- Users should not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or the School.

Personal Use of Social Media:

Students and members of the wider school community should not identify themselves as members of UIS in their personal web-space, unless specifically linked to an approved job role within the school community where it serves a purpose to professionally market the school. This is to prevent information linked with the school and to safeguard the privacy of staff members, students and parents and the wider school community.

- Students should not have contact through any personal social medium with any member of staff, whether from UIS or any other school, other than those mediums approved by the school.
- If students and members of the wider school community wish to communicate with staff they should only do so through the approved means, typically by email or meeting.
- Information that students and members of the wider community have access to as part of their involvement with UIS including personal information, should not be discussed on their personal web space.
- Photographs, videos or any other types of images of students and their families or images depicting staff members, clothing with school logos or images identifying school premises should not be published on personal or public web space without prior permission from the school.
- School email addresses should not be used for setting up personal social media accounts or to communicate through such media.

All parents, students and members of the wider community are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. All parents, students and members of the wider community should keep their passwords confidential, change them often and be careful about what is posted online.

Students and parents should not post images or videos from school events on any public social media site unless permission is sought by the school.

Sites like LinkedIn may be used for professional purposes to highlight a personal profile with summarised detail. However, the school advises that care is taken to maintain an up-to-date profile and a high level of presentation on such sites if UIS is listed.

Using Social Media

Students should only use official school channels for communicating with staff, or with other students to communicate with one another for the purposes of an educational context. ISAMS and Microsoft365 are the current platforms by which staff and students should communicate and no other medium should be used without careful consideration.

The school is responsible for running its official website. No other social media platforms may be set up by any member of the whole school community which have a direct or indirect connection with School.

Use of certain media is permissible during school hours by students, provided permissions are sought and granted in accordance with the school policy.

Monitoring of Internet Use

UIS monitors the use of its internet, online content, online services and email services without prior notification or authorisation from users. Users of email and internet service should have no expectation of privacy in anything they create, store, send or receive using the school's ICT system. All students and members of the wider school community should refrain from downloading unauthorised, unwarranted or inappropriate content using the school's internet or Wi-Fi.

Breaches of this Policy

Any breach of this policy that leads to a breach of confidentiality, defamation, or damage to the reputation of UIS or any illegal acts or acts that render the school liable to third parties may result in legal action, disciplinary action or sanctions in line with the published school policies.

TAALEEM ACCEPTABLE USE POLICY/BRING YOUR OWN DEVICE POLICY – APPENDIX 4

The Rationale:

The focus of the Acceptable Use Policy (AUP) / Bring Your Own Device (BYOD) policy at Taaleem Schools is to provide tools and resources to the 21st Century Learner. Excellence in education requires that technology is seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future. The AUP/BYOD policy is a way to empower students to maximize their full potential and to prepare them for college and the workplace. Learning results will improve from the continuous dynamic interaction among students, educators, parents and the extended community. Technology immersion does not diminish the vital role of the teacher. To the contrary, it transforms the teacher from a director of learning to a facilitator of learning. Effective teaching and learning with wireless technology tools integrate technology into the curriculum anytime, anyplace. The policies, procedures and information within this document apply to all wireless mobile devices used at Taaleem Schools, including any other device considered by the Administration to come under this policy. Teachers may set additional requirements for use in their classroom.

BYOD includes all Mobile devices and any wearable technology

BYOD, while not school property, also fall under the Acceptable Use Policy whilst on school property or whilst on school related activities. However, the school is not responsible for the repairs, loss or theft or any damage resulting from their use on school property or during school related activities. Improper use of BYOD will lead to immediate confiscation and permanent denied access to the school Wi-Fi network. The devices will only be returned the parents or legal guardians of the student owning the device.

Social Media

Due to the wealth of new social media tools available to students, student products and documents have the potential to reach audiences far beyond the classroom. This translates into a greater level of responsibility and accountability for everyone. Below are guidelines that students should adhere to when using Web 2.0 tools in the classroom:

1. Be aware of what you post online. Social media venues including wikis, blogs, Edmodo, twitter, Facebook, Instagram and photo and video sharing sites that are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you would not want friends, enemies, parents, teachers, or a future employer to see.

2. Follow the school's code of conduct / behaviour policy, when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.
3. Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birthdates, and pictures. Do not share your password with anyone besides your teachers and parents.
4. Linking to other websites to support your thoughts and ideas is recommended. However, be sure to read the entire article prior to linking to ensure that all information is appropriate for a school setting.
5. Do not use other people's intellectual property without their permission. **It is a violation of copyright law to copy and paste other's thoughts.** When paraphrasing another's idea(s) be sure to cite your source with the URL. It is good practice to hyperlink to your sources.
6. Be aware that pictures may also be protected under copyright laws. Verify you have permission to use the image or it is under Creative Commons attribution.
7. How you represent yourself online is an extension of your personal image. Do not misrepresent yourself by using someone else's identity.
8. Blog and wiki posts should be well written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work be sure it is in the spirit of improving the writing.
9. If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell your teacher right away.
10. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or access to future use of online tools.

Taking Care of school mobile devices

Taaleem Schools may provide users (staff and students) with mobile devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to Staff/IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

School mobile devices that are broken or fail to work properly at the time they are in the custody of the students or staff must be taken promptly to the Staff/IT technician for an evaluation of the equipment.

General Precautions

- School mobile devices are school property and all users will follow this policy and the acceptable use policy for technology.
- Only use a clean, soft cloth to clean the screen, no cleansers of any type.
- Cords and cables must be inserted carefully into the mobile device to prevent damage.
- School mobile devices must remain free of any writing, drawing, stickers, or labels.
- School mobile devices left unsupervised are at the users own risk.
- For personal devices parents must ensure their child's mobile device comes to school fully charged and loaded with Apps requested by the school.
- Students below grade 3 should never to take the Mobile devices outside the classroom.
- Do not leave the mobile device in an open carry bag so as to prevent it from falling out or from theft.

Carrying Mobile devices

The protective cases provided with mobile devices have sufficient padding to protect the mobile device from normal treatment and provide a suitable means for carrying the device within the school. The guidelines below should be followed:

- School mobile devices must always remain within the protective case when carried.
- Only one mobile device should be carried at any one time.
- Class sets of mobile devices must be carried in the mobile device trolley.

Screen Care

The mobile device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the mobile device when it is closed.
- Do not place anything near the mobile device that could put pressure on the screen.
- Do not place anything in the carrying case that will press against the cover.
- Clean the screen with a soft, dry cloth or anti-static cloth.

- Do not bump the mobile device against lockers, walls, car doors, floors etc as it will eventually break the screen.

Using Mobile and BYOD devices at School

Mobile devices and BYOD devices are intended for use at school each day. In addition to teacher expectations for Mobile device and BYOD use, school messages, announcements, calendars and schedules may be accessed using the mobile device and BYOD. The mobile device or BYOD cannot be used unless a teacher has given permission for its use.

Screensavers/Background photos/Apps

The screensaver or background photo may not be changed for any reason on any school mobile devices. Any changes to the display of the school mobile device will be deemed a violation of this policy. Passwords are not to be used on school mobile devices. Inappropriate material or photos are not to be stored on school or BYOD. BYOD containing material considered inappropriate by the school will be confiscated and returned only to a responsible adult. The device may not be brought to school until the offending material/Apps are removed.

Sound, Music, Games, or Programs

- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Music and Internet Games on the school mobile devices are allowed at the discretion of the teacher.
- If game apps are installed on school mobile devices, it will be by school staff only.
- All software/Apps must be school provided (school mobile devices only).
- All Apps on BYOD are the financial responsibility of the student's family. School required Apps must be installed and updated at home.

Printing

Printing will not be immediately available for students with school mobile devices or BYOD

Saving to the Mobile device/Home Directory

Students may save work to OneDrive - Students are responsible for ensuring adequate back up of their work. BYOD owners must not store personal information on the school acquired third party storage area to avoid any privacy issue violation.

Network Connectivity

Taaleem Schools makes no guarantee that their network will be up and running 100% of the time. In the rare case that the network is down, the Taaleem school will not be responsible for lost or missing data.

Originally Installed Software

The software/Apps originally installed by Taaleem school must remain on the school Mobile device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular course. The licenses for this software require that the software be deleted from mobile devices at the completion of the course. Periodic checks of school mobile devices will be made to ensure that students have not removed required apps. Parents assume the responsibility for all software stored on BYOD devices.

Additional Software

Students are not allowed to load extra software/Apps on the school mobile devices. School mobile devices will be synchronised so that they contain the necessary apps for schoolwork. BYOD users may have to install software at home at the family's discretion and expense.

Inspection

Students may be selected at random to provide their device for inspection including BYOD to ensure that there are not any violations to this policy.

Procedure for re-loading software

If technical difficulties occur and illegal software or non-School installed apps are discovered, the school mobile device will be restored from backup. The school does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.

Software upgrades

Upgrade versions of licensed software/apps are available from time to time. Mobile devices may be removed from circulation for periodic updates and synching. All BYOD devices are expected to update software at home and not during the school day.

Acceptable Use

The use of School technology resource is a privilege, not a right. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges will be terminated, access to the school's technology resources will be denied, BYOD devices will be denied access to the network and WiFi facilities and the appropriate disciplinary action shall be applied. The school code of conduct/behavior policy shall be applied to student infractions.

Violations may result in disciplinary action up to and including suspension/ expulsion for students. When applicable, law enforcement agencies may be involved after KHDA/ADEC consultation

Parent/Guardian Responsibilities

Parents have a responsibility to talk to their children about values and the standards that their children should follow regarding the use of the Internet as they would in relation to the use of all media information sources such as television, telephones, movies, radio and social media. Parents may opt out of allowing their child to use the school mobile devices or BYOD. To opt out parents must sign a form indicating this and acknowledging that their child is still responsible for meeting the course requirements (*which may take longer*).

School Responsibilities are to:

- Provide Internet and Email access to its students.
- Provide Internet Blocking of inappropriate materials where possible.
- Provide access to cloud storage within the school's MS domain.
- The school reserves the right to review, monitor, and restrict information stored on or transmitted via school owned equipment and BYOD devices and to investigate inappropriate use of resources.
- Provide staff guidance to aid students in doing research and help assure student compliance of the acceptable use policy.

Students are Responsible for:

- Using computers/mobile devices in a responsible and ethical manner.
- Obeying general school rules concerning behaviour and communication that apply to Technology equipment use.

- Using all technology resources in an appropriate manner so as to not damage school equipment. This damage includes but is not limited to the loss of data, resulting from delays, non-deliveries, misdeliveries or service interruptions caused by the students own negligence, errors or omissions.
- Use of any information obtained via the school's designated internet system is at your own risk. The school and Taaleem specifically denies any responsibility for the accuracy or quality of information obtained through its services.
- Helping the school protect our computer system/device by contacting an administrator about any security problems they may encounter.
- Monitoring all activity on their account(s).
- Students should always turn off and secure the mobile device and BYOD devices after they are done working to protect their work and information.
- If a student should receive an email containing inappropriate or abusive language or if the subject matter is questionable, he/she is asked to print a copy and turn it in to the office.
- Returning the school mobile device to the class monitors at the end of each period/s or day.
- Ensuring all BYOD devices are fully charged at the start of the school day.
- Their BYOD device is brought to school each day unless otherwise informed.
- Ensure their BYOD device has the Apps/software installed as requested by the school and maintain software upgrades.

Student Activities Strictly Prohibited:

- Illegal installation or transmission of copyrighted materials,
- Students must not take pictures or movies of students who have not given their permission to do so,
- Any action that violates existing school policy or public law,
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, religious or sexually explicit materials,
- Use of chat rooms, sites selling term papers, book reports and other forms of student work,
- Internet/Computer Games without permission of the school,
- Changing of school mobile device settings (exceptions include personal settings such as font size, brightness, etc),
- Downloading apps at school unless supervised by the teacher and parental consent.
- Spamming-Sending mass or inappropriate emails,
- Gaining access to other student's accounts, files, and/or data,
- Use of the school's internet/E-mail accounts for financial or commercial gain or for any illegal activity,
- Use of anonymous and/or false communications such as MSN Messenger, Yahoo Messenger,

- Students are not allowed to give out personal information, for any reason, over the Internet. This includes, but is not limited to, setting up internet accounts including those necessary for chat rooms, EBay, email, etc.,
- Participation in credit card fraud, electronic forgery, or other forms of illegal behaviour,
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed,
- Bypassing the School web filter through a web proxy.

Mobile device and BYOD Care

- Students will be held responsible for maintaining their own devices and keeping them in good working,
- order whilst in their possession,
- BYOD devices must be recharged and ready for school each day,
- The school will be responsible for repairing only school owned Mobile devices that malfunction,
- Mobile devices that have been damaged from student/staff misuse or neglect will be repaired with,
- cost being borne by the student/staff. In the event of an accidental damage, the school on a case-to-case,
- basis may exercise discretion in recovering the cost of repair to the device from the user.

Mobile device theft

- Mobile devices that are stolen must be reported immediately to School SLT/Principal and may require further reporting to the local Police.

Legal Propriety

- Comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity.
- Plagiarism is a violation of the School code of conduct / behavior policy. Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.
- Use or possession of hacking software is strictly prohibited and violators will be subject to consequence as stipulated in the School Parent/Staff Handbook. Violation of applicable law will result in criminal prosecution or disciplinary action by the school.

Protecting & storing of the Mobile and BYOD devices

Mobile devices and BYOD will be labelled in the manner specified by the school. Mobile devices can be identified and located in the following ways:

- Record of serial number
- Identification label

All school Mobile devices shall be stored in the Mobile device trolley and locked. All BYOD devices must be clearly labelled with the owners name and grade/class. All BYOD devices must be taken home each night.

AUP/BYOD User Pledge

1. I will only use the School facilities, equipment and Internet when these are officially available for my use.
2. I will only access my account and make sure no one else has access to my account. I understand that I am responsible for all actions that take place on my user account.
3. I will not download, transfer, write, draw or view any unsuitable graphic, text or other inappropriate material and it is my responsibility to immediately inform the teacher should I accidentally access anything inappropriate.
4. I will not download, transfer, install or use any applications, utilities, games, music, video files or other files or software not approved by the School.
5. I will only go to sites on the acceptable website list unless otherwise directed by my teacher.
6. YouTube, gaming sites, and social networking sites are expressly forbidden unless authorised.
7. I will not partake in any type of cyberbullying and I will report any cyberbullying to a staff member.
8. I will treat the School computers, systems and the school network with respect and care.
9. If I know of someone misusing anything, I will report this to a member of staff anonymously.
10. I will only access the local server or wider network that is readily available to me.
11. If I use any material from the Internet in my own work, I will clearly state the source.
12. I will reduce printing waste by not printing drafts but only final copies and utilising recycled paper where appropriate.
13. I will only use e-mail, chat or messaging facilities during lessons if allowed.
14. I will only use the schools network for transmission and reception of material that would be considered acceptable by the school
15. I will only use my school e-mail address responsibly and appropriately at all times.
16. I will not eat or drink whilst using the ICT facilities and equipment.
17. I will not interfere with the work of others.

18. I will not attempt by any means to circumvent the restrictions placed upon the machine or the network I am connected to.
19. I understand that trying to bypass the blocking put in place by the Telecommunications Regulation Authority (TRA) is against the law of the UAE and will not attempt to do so.
20. I never attempt to “jailbreak” the school Mobile device or attempt any repairs.
21. I will not place decorations (such as stickers, markers, etc.) on the school Mobile devices. I will not deface the serial number Mobile device sticker on any Mobile device.
22. I understand the school Mobile device remains the property of the School.

The following applies for BYOD devices

1. I will take good care of my BYOD device.
2. Students will not use devices on school transport, in public areas of the school, during the school day, unless permitted.
3. I will only use my device for educational purposes as and when requested.
4. I will never leave the BYOD device unattended.
5. I will never loan out my BYOD device to other individuals.
6. I will keep food and beverages away from the BYOD device since they may cause damage to the device.
7. I will use the BYOD device in ways that are appropriate, meeting School expectations.
8. Students understand that the BYOD device is subject to inspection at any time without notice.
9. I will ensure that anti-virus and anti-malware software is installed on my BYOD and is kept updated regularly and frequently.
10. I understand that my personal device is my responsibility and School is not responsible for any breakages, lost, theft or any damage caused by malware on the network
11. I will follow the policies outlined in the Taaleem School BYOD/Acceptable Use Policy.