



MISY | Mandalay

Myanmar International School Yangon (Mandalay Campus)

Myanmar International School of Yangon (Mandalay Campus)

Technology User Policy

Approved by: Nu Nu Aye (BOD)

Date: November 2019

Last reviewed on: June 2024

Next review due by: June 2026



MISY MANDALAY

TECHNOLOGY USER POLICY AND AGREEMENT: EMPLOYERS, STAFF AND VOLUNTEERS

Information and Communication Technology (ICT) is a necessary and expected part of our daily working lives at MISY.

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff and volunteers are expected to sign the agreement based on the policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head of school.

Application

This policy applies to employers, employees and volunteers at the school and in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software, school telephones, cameras and recording equipment, intranet and any other electronic or communication equipment used for work purposes.

This policy also provides advice to employers, members of staff and volunteers in respect of the potential risks and consequences relating to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

Access

Access to ICT facilities is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents unless express permission has been provided. Where staff are able to access email outside of school hours the email facility should not routinely be used to undertake school business outside of reasonable working hours.

Communications to students is occasionally necessary in some areas of the school, however should only be done through the school's accepted avenues of communication and should maintain an exceptional standard of professionalism within the communication. Whilst it is acceptable to communicate with students and parents electronically, it must be done so with forethought and professionalism.

Access to certain software packages and systems will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required and requested for updating of software, licences and virus protection and for verification of the existence and condition of the equipment. Staff with such devices must ensure that any sensitive information is protected accordingly if working outside of the school premise.

Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where images of students are taken, staff must ensure that prior consent has been provided by parents, and that the school's policy in relation to use of pictures, is followed. No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

Communication with parents and students

School telephones – all teachers, administrative staff and staff who have been permitted through specific roles are able to communicate with parents by telephone. Other staff would normally need to seek approval from a senior leader where they feel they need to make a telephone call to a parent

Text/App system– Office staff only. Where other staff need to send a text, this would normally be approved by a senior leader.

Letters –All letters require approval by a senior leader before being issued.

Email – school email accounts should not be used for communication with parents unless approved by a senior leader. Staff must not use personal email accounts for communicating with parents or students. If for any reason a parent initiates a communication to your work email, this should be forwarded to the senior leader of your section

Under normal circumstances staff should not be using **any** methods other than the schools accepted systems, such as Google for Education or Managebac to communicate with students. If a member of staff needs to contact a student directly using anything other than the accepted school communication system, this must be approved, in advance, by a senior leader. Approval for any other form of contact to meet lesson based needs e.g. closed Facebook groups, must be sought, in advance from a senior leader.

Staff should not engage in communications with students via personal lines of communication such as text messages, social media messaging platforms or private emails.

Social networking

School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

Under no circumstances should any school staff have any students or any ex-students under the age of 18 as friends on their social networking sites. School staff are strongly advised not to have any online friendships with any young people (i.e. including those at other schools) under the age of 18, unless they are family members.

Where school staff do accept friendships via their social networking with ex-students aged over 18, they are advised to notify a senior leader. Staff in secondary schools are strongly advised to exercise care and consideration before accepting online friendships with ex-students aged under 21. This is particularly relevant where the students have left the school recently or the student or

their family have an ongoing relationship with the school (e.g. they have siblings that continue to attend the school).

School staff are strongly advised not to accept friendships via their social networking with parents or ex- parents. Where staff do accept such friendships, they must not engage in any discussion regarding individual students or the school, whether expressing personal views or opinions or simply recounting events or stating facts.

School staff are able to accept friendships with colleagues via their social networking site but should take care in communications exchanged. It is important that this avenue of communication is equally respected, similarly to the lines of communication used in the workplace. Should issues arise between staff in a communicative form on social media, it is possible that senior leadership may have to take these into consideration when dealing with this grievance.

Where the school uses social networking sites as a means of communication with the school community, school staff must follow the guidance provided by the school in the use of the sites. It is expected that staff either do not show or show a positive and supportive attitude towards the school in the social media environment.

No photos of students should be posted on social networking sites.

Where school staff become aware that there is information about them held on social networking sites that causes them personal concern, they should alert a senior leader to their concern.

Unacceptable use

School time, systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share
- to promote political or religious, or extreme viewpoints in any capacity or forum
- to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others
- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material
- to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally or to post such material online.
- to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its students, or to share support of such views that may already have been promoted in an online environment.
- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy, limit the functionality of or hold to ransom any computer software or hardware or telecommunications equipment
- to collect or store personal information about others without permission from senior leaders.
- to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project
- to visit or use any online messaging service, social networking site, chat site, web based

- email or discussion forum not supplied or authorised by the school
- to undertake any activity (whether communicating, accessing, viewing, sharing, uploading or downloading) which has negative implications for the safeguarding of children and young people

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a senior leader.

Where an individual accidentally accesses a website or material that they consider to be pornographic or offensive or otherwise inappropriate, this should be reported immediately to a senior leader.

Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to a senior leader so that this can be dealt with appropriately.

Personal and private use

All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this access is not:

- taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)
- interfering with the individual's work
- relating to a personal business interest
- involving the use of news groups, chat lines or similar social networking services
- at a cost to the school
- detrimental to the education or welfare of students at the school

Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time can have implications for their employment situation. Where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people action will be taken.

Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by students at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, approval must be sought in advance from a senior leader and staff should take care to ensure any school data/images are deleted following use of the equipment.

Security and confidentiality

Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

School staff must take account of any advice issued regarding what is permitted in terms of

downloading educational and professional material to the school server. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to a senior leader.

Where staff are permitted to work on material at home and bring it in to upload to the school server through their memory pens, they must ensure that they have undertaken appropriate virus checking on their systems. Alternatively, staff are encouraged to store their data on Google Drive where they can access this from home.

Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals. This is particularly important when using data off site. Electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens and only then after permission from a senior leader. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

Monitoring

MISY reserve the right to monitor the use of all aspects of any user including but not limited to email, internet use and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

- to ensure that the security of the school's hardware, software, networks and systems are not compromised.
- to prevent or detect crime or unauthorised use of the school's hardware, software, networks or systems
- to gain access to communications where necessary where a user is absent from work

Where staff have access to the internet during the course of their work, it is important for them to be aware that the school may track the history of the internet sites that have been visited, even with the use of 'private browsing'. Whilst this list is long, it is not at all exhaustive and any arising concerns or situations will be dealt with on a case by case basis by senior leadership where it is deemed necessary to do so by the school.

Signature

Staff are to read and sign the acceptable use agreement, to confirm that they have had access to the Technology Use Policy and that they accept and will follow the terms.

Linked policies:

Data protection policy

Safeguarding Policy

Technology user agreement

Staff handbook

Appendix 1 Technology user agreement: staff

Myanmar International School of Yangon Technology User agreement for staff

- I appreciate that ICT includes a wide range of systems, including mobile phones, personal digital assistants, cameras, email, internet, intranet access and the use of social networking. ICT use may also include personal ICT devices when used for school business.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private use without the permission of a senior leader.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy.
- I understand the level of authority required to communicate with parents and students using the various methods of communication.
- I understand that I must not use the school ICT system to deliberately access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, harassing or bullying is an inappropriate use of ICT.
- I understand that if I were to share my name, address, credit card or bank details etc. on the internet in school, I am doing so at my own risk and the school accepts no responsibility.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I understand that images of students and/or staff will only be taken, stored and used for professional purposes. Images will not be distributed outside of the school network without the written permission of the parent/carer, member of staff or senior leader.
- I will respect copyright, intellectual property and data protection rights.
- I understand that use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to a senior leader.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with students, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I understand that personal details, such as mobile phone numbers and personal email addresses should not be given to students.
- I will promote e-safety with students in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known, and that activities undertaken are inconsistent with expectations of staff working with children.
- I will ensure that my laptop/workstation is locked if I leave it unattended.
- The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound. I understand this agreement forms part of the terms and conditions set out in my contract of employment.
- I understand that staff are more than welcome to access and work outside of the normal working hours if they wish, but this is not an expectation. Equally, it is not expected for staff to read or respond to communications received outside of normal working hours.

User's signature

I agree to follow this agreement and to support the safe and secure use of ICT at Myanmar International School Yangon.

Full Name (Block capitals)

Job Title (Block capitals)

Signature

Date (Day/Month/Year)

Appendix 2: Technology user agreement: Secondary students

Myanmar International School of Yangon Technology User Agreement for students in Years 7-13

School intranet

- I understand that ICT systems in school, including the internet, email, digital video, mobile technologies are for school purposes only.
- I will not download or install software on school technology equipment.
- I will only log on to the school network with my own username and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will not take a disk or CD from school nor copy school software to install at home.
- When using external flash drives I will get the ICT department to scan these for viruses before using them in the school computers.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

World-wide web

- I will be *responsible* for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload, or forward material (including images) that could be considered offensive or illegal, hateful or otherwise objectionable. If I accidentally come across any such material I will report it immediately to a teacher.
- I will use the internet for educational purposes only.
- I understand that among the valuable content online there may also be unverified, incorrect, or inappropriate content and I must be careful before using the same in my homework or research.
- I will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- If I believe a school computer I am using might be infected with a virus, I will alert my teacher.
- I will check twice before clicking on anything I feel is not right.
- I realise certain websites may be blocked and will not attempt to bypass the internet filtering system.
- I understand that any usage, including distributing or receiving information, school-related or personal, may be monitored and logged and can be made available to my teachers especially for unusual activity, security and/or network management reasons.
- I understand that these rules are designed to keep me safe and that if I do not follow them school sanctions will be applied and my parent/ guardian will be contacted.

E-mail, internet communication, social networking and personal safety

- While in school I will not use email for personal reasons; only for educational purposes and by using approved email addresses as authorised by my teacher.
- I will only open email attachments from people I know.
- While in school I will not access Facebook, Twitter, Instagram, Snapchat, YouTube, Discord, TikTok etc without permission.
- I will not use language online that would be unacceptable in the classroom.
- If I see a message, comment, image, or anything else online that makes me concerned for my personal safety, I will bring it to the immediate attention of a teacher if I am at school or a parent / guardian if I am at home.
- I will never share or publicise personal information such as my name, birth dates, phone number, home address or pictures.
- I will not reveal other people's personal details, such as addresses or telephone numbers or pictures.
- I will not arrange to meet someone I only know through emails or other online communication.
- I will not post anything online that I would not want parents, teachers, or future colleges or employers to see.
- I will not post anything online which brings the school into disrepute or is critical of the school.
- I will not attempt to access sites, servers, accounts, or content that isn't intended for my use.
- Images of students and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network.

Cyber-bullying

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could physically or emotionally frighten, hurt or bully someone else.
- I will not use another person's identity to trick or fool.
- I will not send or receive any material that is illegal, obscene and/or defamatory.
- I understand that in some cases, cyber-bullying is a crime and that the school will support students, teachers and parents in dealing with this offence.
- I will respect the privacy and ownership of others' work online at all times.
- I understand that any work that I submit as my own can be verified by staff using plagiarism checkers, and that plagiarism (trying to pass someone else's work off as my own) is an offence.

Student personal devices: Mobile phones, laptops, tablets, iPods, cameras, etc.

- I understand that these personal devices are not to be used on school premises unless authorised by a teacher and only at appropriate times, in approved places, for learning reasons.
- I will ensure all such devices are SWITCHED OFF in the school building. Devices in 'Silent' or 'Vibrate' mode are not considered 'off'.
- I may use these devices for emergency purposes (with permission from the teacher).
- I will not connect or attempt to connect to the school's network system (wired or wireless) without permission.
- I understand that noncompliance will result in confiscation of the above mentioned devices.
- I know that my use of ICT will be checked and that my parent/guardian will be contacted if the school has reason to be concerned about my safety. This may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion.
- I also understand that the school also reserves the right to monitor my use of school technology systems and report any illegal activities to the appropriate authorities.

User Signature:

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout Myanmar International School Yangon.

Full Name(printed)

Tutor group(printed)

Signature

Date

Appendix 3: Technology user agreement primary students

Myanmar International School of Yangon Primary technology user agreement for students

Primary school profile statement

At MISY we support the right of all members of the school community to access safe and inclusive learning environments, including digital and online spaces. This form outlines the Primary school's roles and responsibilities in supporting safe digital learning, as well as the expected behaviours we have of our students when using digital or online spaces.

In primary we will:

- Educate our students about digital issues such as online privacy, intellectual property and copyright;
- Supervise and support students using digital technologies in the classroom;
- Use clear protocols and procedures to protect students working in online spaces. This includes reviewing the safety and appropriateness of online tools and communities, removing offensive content at the earliest opportunity.
- Use online sites and digital tools that support students' learning.
- Address issues or incidents that have the potential to impact on the wellbeing of our students.
 - Refer suspected illegal online acts to the relevant Law Enforcement authority for investigation.
- Support parents and care-givers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home.

Expected Student behaviour when using digital or online spaces.

To encourage safe, responsible and behaviour

When I use digital technologies I **communicate respectfully** by:

- Always thinking and checking that what I write or post is polite and respectful.
- Being kind to my friends and classmates and thinking about how the things I do or say online might make them feel.
- Not sending mean or bullying messages or forwarding them to other people.
- Creating and presenting my own work, and if I copy something from online I show people where I copied it from by writing the website link.

When I use digital technologies I **protect personal information** (which is my full name, photo, birthday, address and phone number), and know that it is not to be shared online. This means I:

- protect my friends' information in the same way
- protect my passwords and don't share them with anyone except my parent
- only ever join spaces with my parents or teacher's guidance and permission
- never answer questions online that ask for my personal information
- stop to think about what I post or share online

When I use digital technologies I **respect myself and others** by thinking about what I share online. This means I:

- use sites that are appropriate, and if I am not sure I ask a trusted adult for help
 - speak to a trusted adult if I see something that makes me feel upset or if I need help.
 - speak to a trusted adult if anyone asks if anyone I've met online asks me to meet them in real life.
 - speak to a trusted adult if someone is unkind to me or if I know someone else is upset or scared
 - don't deliberately search for something rude or violent
 - turn off or close the screen if I see something I don't like and tell a trusted adult
 - I am careful with the equipment I use.
 - will not write bad comments about the school online.

When I use **school equipment I will be respectful.**

This means I:

- Only use school computers to help my learning.
- Only look at and work on my own files
- Keep all school equipment at school and not take any home
- Will ask the teacher to scan any external flash drives (USB) before I use
- Will tell a teacher if I think a school computer has a virus
- Only use the school network with permission from a teacher.

When I communicate with others using email or social media **I will protect myself** by:

- Only using email for learning purposes
- Not using social media sites underage (Twitter, Facebook, Snapchat, Instagram, YouTube etc.)

When I use my own personal device I will **use it responsibly.**

This means I:

- only use my personal device when given permission by a teacher or in an emergency situation. If I am not using it for learning it must be switched off at all times. (not in silence or vibrate)
- If I am using my own device when I should not, it may be taken by a teacher.

I understand that the teachers may check that I am using technology correctly according to this agreement. If I do not follow this agreement my parents may be contacted and I may not be able to use technology at school.

Student name: Signature.....

Parent name:..... Signature:.....

Class:..... Date:.....