Myanmar International School Yangon

TECHNOLOGY USER POLICY AND AGREEMENT: EMPLOYERS, STAFF AND VOLUNTEERS

Approved by:	Ei Ei Zin (Board of Directors)	**Date:**
Last reviewed on:	26th October 2022	
Next review due by:	26th October 2024	

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.

Electronic communication with students is sometimes necessary, however, it should only be undertaken through the school's accepted avenues of communication and should be undertaken in a professional manner.

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, licenses 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, 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 libelous, 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 posts 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 unauthorized 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 Technology user agreement, to confirm that they have had access to the Technology Use Policy and that they accept and will follow the terms and conditions.

Linked policies:

Data protection policy

Safeguarding Policy

Technology user agreement