The School has placed restrictions on what can be accessed using the School’s ICT Systems. This document has been prepared to explain what the expectations are for anyone using the School’s ICT systems (Computers, Laptops, Email, Internet, Intranet, Moodle and, Wi-Fi Access etc).

**Some guiding principles –**

- All users of DSC ICT Systems are required to sign an Acceptable Use Agreement.
- The School’s ICT system and resources must only be used for educational purposes.
- The School will monitor usage of School systems with automated and manual checks of logs and traffic.
- The use of the School’s ICT systems is a privilege, not a right.
- Inappropriate use will result in the cancellation of ICT privileges and possible other disciplinary action.
- School Administration will decide what inappropriate use is.
- The School will audit all School Systems for policy violations.
- The School will cooperate with government officials concerning any illegal activities conducted through the School’s ICT systems.
- The School may report serious or criminal activities to the Computer Crimes Unit of the Hong Kong Police Department.
- The School may report serious copyright violations to the appropriate agencies.
- Users will not attempt to access another user’s account.
- Users are accountable for access to the system by his or her account.
- Passwords are to be kept safe, secret and secure.

**Privacy Expectation –**

- Users should have limited privacy expectations when using the ICT systems at the School. The School will attempt to keep the contents of personal folders and email secure and confidential. Users need to be aware that privacy on the ICT Systems is not absolute.
- The School cannot guarantee the confidentiality of information stored on the network or School systems. This information may be seen by authorized personnel as they are carrying out routine maintenance, answering a service call, or other job related tasks.
- User access of the School’s ICT systems requires a user account. This will enable individual users to be identified and his or her access traced.
- Students will be identified only by his or her first name on Internet sites accessible by the public.
- Students may be identified by his or her first and last name on School internal (private intranet) sites.
- Users will not disclose personal contact information over the School’s systems.
- Users will not disclose names and personal contact information about other students over the ICT systems.
- Users will not forward a message that was sent to them privately without permission of the
person who sent them the message

Technology Protection Measures –

The School has set up several technology protection devises to help secure the ICT systems used by students. These systems include a web filter, an email SPAM and profanity filter, a firewall, and anti-virus systems. These systems remain on at all times when users are accessing internal and external resources. The log files and alerts produced by these systems can be used to identify inappropriate use of the School’s ICT systems.

Plagiarism and Copyright Infringement –

It is the aim of the School that all students respect and follow laws protecting copyright material. The School does not condone the illegal use or reproduction of material protected by copyright. Students who willfully disregard this policy do so at their own risk and assume all liability.

- Students own the copyright to the work they create.
- Student work will only be posted on the School website and Moodle with the permission of the student.
- Users will not plagiarize works that they find on ICT Systems.
- Users will respect the rights of copyright owners in their use of materials found on, disseminated through, or posted to ICT Systems.
- No School hardware can be used in a manner that would infringe upon the rights of a copyright holder.
- No material may be distributed through the School’s ICT systems or posted on the School’s ICT Systems unless that material is original or when posted with permission of the copyright owner.
Email Usage and Monitoring Policy -

The School provides email accounts to users primarily for the communication between students and staff. The School does allow reasonable and responsible use of email accounts for non-school or personal purposes on the expressed understanding that such usage will be appropriate. The School’s email policy must be followed. If the email policy is not followed the user will have his or her email account closed.

Email Acceptable Use Policy - The following uses of Email are not permitted:

- sending defamatory or indecent messages (containing obscene, profane or rude language)
- sending or distributing unlawful materials
- distributing or sending personal data (name, address, phone number, assessment marks, etc) about other people
- distributing or sending sensitive or confidential information
- distributing or sending unsolicited bulk mails or data that function in a malicious manner
- performing any unlawful activities
- sending SPAM messages, chain letters or mass emails
- harassing another user or person
- checking or replying to email messages while in class, unless given permission by the teacher
- forwarding a message without permission of the person who sent the message

Excessive use of email by a user may raise a reasonable suspicion that the user is using electronic mail in violation of School Policy.

Respecting Privacy Rights –

- Student users must not intercept email communications meant for others.
- Student users must not assist others in intercepting email communications meant for others.

The School is committed to respecting the reasonable expectation of privacy by its ICT users. The School also is responsible for operating, maintaining, and protecting its ICT systems. To accomplish this it is occasionally necessary to intercept or disclose email messages. The School may use content monitoring systems, message logging systems, or other tools. By using the School’s systems, users consent to permit all information they store on the School’s systems to be divulged to law enforcement agencies or reviewed, if suspected of acceptable use violations, at the discretion of the School.

No guarantee of message privacy -

The School cannot guarantee that email messages will be private. Email can be forwarded, intercepted, printed, and stored by other people. Email messages can be accessed by people other than the intended recipients. Because messages can be stored in backups, electronic communications actually may be retrievable when a traditional paper letter would have been discarded or destroyed. Be very careful about the topics covered in email messages.

Content of messages may be scanned by the Email System

Sexual, ethnic, and racial harassment is strictly prohibited. Users must not use profanity, obscenities, or derogatory remarks in email messages. As a matter of standard practice, all School electronic communications must be consistent with conventional standards of ethical and polite
conduct. Users who receive offensive unsolicited material from outside sources or another user should report the incident to the IT Department.

The Global Address List (Found in Outlook) –

This address book contains the email addresses of all users. It is provided by the School to students and staff only. Users may use the address book to look up email addresses of school members for communication purposes. It is the responsibility of all students and staff to keep the information securely and on no account must it be shared with anyone who is not on the list.

Statistical Data -

The School may collect statistical data about its email system. Using such information, technical support personnel monitor the use of electronic communications to ensure the ongoing availability, reliability, and security of these systems. The School may employ computer systems that analyze these types of statistical information to detect unauthorized usage, denial of service attacks, and other problems.

Purpose of Monitoring Email Usage –

The School may use automated software to keep and monitor logs of email usage for the following purposes:

- to facilitate the efficient provision of service to customers;
- to maintain a stable email service environment for communications;
- to provide information for management to ensure the proper utilization of company’s resources;
- to ensure the compliance of users with DSC’s email usage and Personal Data Protection policies.

Email Scanning and Monitoring

Every email message that passes through the server will be scanned for computer viruses, worms, and executable files that could pose a threat to the security of the network. Infected email will be deleted.

The School shall scan the content of every email message that passes through its servers based on a predetermined criterion. If the message does not pass the criteria, the message will not be delivered to the user.

The School reserves the right to log all out-going and in-coming emails. The email log contains the email addresses of the sender or recipient, the date, time, and message header information. Copies of emails are also stored in network mail servers. The School reserves the right to access the contents of all School-related emails held in a user’s mailbox(es), at any time, even during periods when users are absent from work. Random checks may be conducted to ensure the conditions of use of email facilities are observed.
Acceptable Use Policy -

DSC computers and ICT Systems are to be used in a responsible manner. Likewise, students bringing to campus student-owned device must also use the technology in a reasonable and responsible manner.

In order to ensure a healthy educational environment at DSC the following must be avoided when using technology on Campus:

- playing games on laptops during instructional time
- using a laptop or internet access during class time without the approval of the class teacher
- attempting to gain unauthorized access to the School’s ICT system
- attempting to hack into another person’s computer or computer system
- going beyond authorized access level
- knowingly posting false or defamatory information
- accessing another user's account or files without permission
- disrupting the computer network performance
- destroying data or deleting information that is not your own
- intentionally infecting computers with viruses
- intentionally damaging computers and ICT Systems
- posting information that could cause damage or harm to others if used
- using the School’s System to engage in an illegal act
- engaging in personal attacks, including discriminatory attacks
- sending or displaying offensive messages or pictures
- using internet P2P sites for downloading or accessing material posted on the internet
- making anonymously posting on the School intranet/Moodle or class wiki/portal
- posting any material that is knowingly false, misleading, or inaccurate on the School Systems
- using profanity
- posting content/web link that is obscene, sexually oriented, or sexually suggestive on the School Moodle or class wiki/portal
- posting material without the permission of the copyright owner on the School Moodle or class wiki/portal

Due Process –

All infractions or suspected infraction of the School’s Acceptable Use Policy will be handled in accordance to the School’s Discipline Policy. Details in regards to this Policy may be found in the Student and Parent Handbook.