Information & Communications Technology Acceptable Use Policy For Visitors

Version 1.8

Effective Date
1 Aug 2022

Document Control

Revision History

Version	Date	Description	Author
1.0	23 Mar 2010	Initial Release. Replaces Security Policy Governing the Use of Computer Resources at the Singapore Polytechnic.	EMC Consultant
1.1	1 Nov 2011	Change of password policy to meet password complexity requirement.	Anthony Lau
1.2	1 Aug 2014	Updated to align with change of SP ICT Security Policy & Standard	Deloitte Consultant
1.3	1 Sep 2016	Editorial changes.	Jason Tseng
1.4	28 Nov 2017	Logo and editorial changes. Added inactive accounts will be disabled after 90 days.	Jason Tseng
1.5	1 Apr 2019	Update password policy. Editorial changes.	Jason Tseng
1.6	1 Jul 2020	Editorial changes. Align password policy to AD password policy.	Jason Tseng
1.7	1 Jun 2021	Editorial changes Authorization requirement for bug-hunting/PT/VA	Jason Tseng
1.8	1Jun 2022	Added precaution when reading email (phishing, spoofing)	Jason Tseng

Reviewers

Name	Role	Status
Chairman & Members	ICT Working Committee	Endorsed

Approvals

Name	Title	Date
Chairman & Members	ICT & Digitalisation Steering Committee	1 Aug 2022

Table of Contents

1. Introduction

As a visitor to Singapore Polytechnic, you have been granted access to make use of the Polytechnic's ICT Assets such as information, computers, networks and software for the scope of works engaged by the Polytechnic. It is important that these important resources provide the service to you and to others for which they were intended.

An important part of the proper operation of these ICT Assets is security. Trojans, viruses, worms, spyware and ransomware can wreak havoc on these assets so the Polytechnic has taken great care to protect them against such threat.

This document is intended to explain what you need to do, and what rules you need to comply with to help ensure that the confidentiality, availability and integrity of the computing resources of the Polytechnic are protected.

All visitors of SP are required to strictly comply with the Information Communications Technology (ICT) Security Policy and Standard issued by the Polytechnic.

2. Passwords

You may have been given a password to access computer accounts that you need. You must keep your password secret, and never tell anybody else what it is[1];

To comply with Singapore Polytechnic's ICT security policy:

- It needs to be at least 12 characters long;
- Shall contain characters from at least 3 of the following categories:
  - Upper case (A-Z)
  - Lower case (a-z)
  - Digits (0-9)
  - Special characters (!, $, #, %, etc.)
- Shall not be reused for at least 3 generations;
- It should not be the same as your username or User ID;
- It should not be your name or part of your name;
- It should not contain your NRIC/Passport Number;
- It should not contain or be anything that can be associated with you, e.g. your dog's name or street name;
- Shall not be dictionary, commonly used words or compromised passwords

Take great care when you pick a password. One easy way to pick one you can remember is to think of a phrase. For example, the phrase "I like Ice Cream" could be converted into a password like 1l1ke1cecream by just putting 1 instead of 'I'; this is a very good password. (Don't use this one though!)

Don't write your password down on a piece of paper or put it in a file on a computer. Somebody else could find it.

[1] One really good example of when this rule is important is when you are the potential victim of a phishing attack, where you get an email asking you to reveal your password. A legitimate site or organization will never ever ask you to reveal your password.

If you think someone has guessed your password, or if you accidently revealed it to somebody else, you need to change it immediately.

You will also need to change your password as and when prompted and you can't use the same password again.

3. Your Accounts

If you need access to ICT Systems to do your job, you will have been issued a SPICE account with a unique User-ID and password. It is very important to understand that this account is for your exclusive use only. You must not share your account with anybody else for any reason whatsoever.

- You must always keep your password secret, and never disclose your password to another person for any reason whatsoever
- You are accountable for all use of the account. This includes, but is not limited to:
    - The contents of all email messages emanating from the account;
    - All instant messaging coming from the account;
    - All social networking postings (e.g. Facebook, Twitter) made from the account;
    - All other forms of information uploaded or downloaded from the account.
- You should be mindful of what you transmit to others from the account
- You must not use or attempt to use someone else's account. You also must not try and monitor another person's data
- You must not access, read, copy, amend or delete another person's files or data
- Inactive accounts will be disabled after 90 days.

4. Appropriate Use SP's Computer Resources

The campus networks, including any computer systems or applications that have been granted access to you are tools to facilitate your work engaged by the Polytechnic. These systems should be usable by you just the way they are, and you must not change their configuration or add/modify/remove any software. Use common sense in what you do on these systems - if it feels wrong, it probably is.

You should only use Polytechnic computer systems and the Polytechnic's networks for Polytechnic related activities, within the scope of work engaged by the Polytechnic, and for no other purpose. You should not use these systems for:

- Commercial or financial gain
- Gambling
- Unauthorized storage
- Attacking or hacking Polytechnic or external resources including the following without explicit authorization from SP: bug-hunting, penetration testing, vulnerability and network scanning.
- Installation of malicious software or code
- Disruptive activities to other users of the Polytechnic as a whole

When connecting to the Polytechnic's networks, the Polytechnic has the rights to monitor, control and disclose your Internet activities. This will include the rights to accept, terminate or reject your connections, as well as the rights to monitor and record your surfing activities.

If required, only authorized software shall be installed on the Polytechnic's systems. Authorized software is software that is licensed for use, legally acquired, and approved by the Polytechnic for use. By installing unauthorized software you could inadvertently introduce malicious code and cause great harm to the Polytechnic. You could also break the licensing agreements that the Polytechnic has with various software vendors, and without even knowing it.

Only use resources that are required for the scope of works engaged or allowed by the Polytechnic. Staff computers are for staff and visitors should not use them. If you have a question regarding a computer system's intended use, please ask.

Do not try and circumvent these safeguards, as you will be endangering both the system and other users.

Information that goes on the Internet from the Polytechnic is traceable to the Polytechnic. Do not use the Polytechnic's network to post or email on to public Blogs, social networking sites[2], websites, or any other publicly accessible communication channel, anything that is:

- False and misleading
- Distasteful;
- Objectionable;
- Fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or
- Incite religious or racial intolerance or are otherwise deemed inappropriate
- Prejudicial to the good name of Singapore Polytechnic;
- Illegal as defined under the laws of the Republic of Singapore;

Again, good sense prevails – defamation, pornography, pictures that are disturbing – if you think it's bad, it probably is.

You must not use the Polytechnic's ICT Systems to illicitly exchange[3] or otherwise infringe on the copyrighted intellectual property of others by any means, including but not limited to the use of "peer-to-peer" or "client-to-client" technologies[4], email or FTP. If you have peer-to-peer or client-to-client software on your personal notebook(s), either turn it off or don't connect your computer into the Polytechnic's network.

When you use your personal mobile devices[5], you can only connect them to networks that are allocated specifically for the scope of works engaged by the Polytechnic or for guest use.

You must not run any diagnostic or vulnerability scanning tools on your personal mobile devices while connected to the Polytechnic's networks.

[2] Social networking sites include sites such as Instagram, Facebook, Twitter, Youtube, TikTok and so on.
[3] By "illicitly exchange", we mean exchange without the permission of the copyright owner or exchange in violation of normal "fair use" principles; this generally applies to music, movies, software, and other forms of intellectual property.
[4] Examples include eDonkey, Gnutella and Bit Torrent
[5] Personal mobile devices refer to your handheld computing devices such as notebook(s), tablets, and smart phones.

You must ensure that you have an appropriate anti-malware program installed, operational and up-to-date – before you connect it to the Polytechnic's network. This is to protect both you and other users' computers against malware.

You must ensure that your personal mobile devices are not attached to a second network[6] and Singapore Polytechnic's network at the same time; for example, if you have a USB dongle that facilitates connections to a mobile data network, then you can't use that dongle at the same time as your device is attached to the Polytechnic's network.

5. Email

The Polytechnic may have created a visitor email account for your exclusive use. If so, you are fully accountable for all emails transmitted from your Polytechnic email account so you must ensure that nobody else can access this account.

When you use your Polytechnic email account, you are in effect representing the Polytechnic. You must exercise care and discretion when you send mail and you must not use your Polytechnic email account to:

- Send false/misleading, spam or commercial emails;
- Solicit for political candidates;
- Engage in illegal, unethical or improper activities;
- Disseminate internal email addresses to external mailing lists;
- Conduct personal business

You must always take precaution when reading your email and stay vigilant for phishing, spoofed, unsolicited and malicious email sent to entice you to click on malicious links/attachments or to solicit sensitive information (eg. passwords, one-time-PIN, personal information etc).

6. Security Violations

If you see something that you think might indicate a security problem, malfunction of a security device or program, or a security violation, please promptly report the matter to the staff that you report to or the SPICE Service Desk – it is your responsibility to do so.

If violations, such as presence of malware, are detected on your personal mobile devices, the Polytechnic will reject your connections to the Polytechnic's networks.

If there is an investigation being conducted by the polytechnic relating to system misuse, abuse or a security incident/violation, then you understand that during the course of the investigation the Polytechnic's management has the right to examine your account, emails, user files and personal mobile devices that have been connected to the Polytechnic's networks.

[6] A "Second Network" is meant to be an un-trusted third-party network such as the Internet; the effect of connecting a computer to two networks at the same time is to circumvent protection mechanisms that may be in place on the trusted network. A good example of connecting to a second network is at the same time would be to connect to the SPICE network using a LAN port while at the same time being connected to Wireless@SG on the Wi-Fi port.

You also understand that violation of the Polytechnic's computer security policy and acceptable use policy is a very serious matter. Violations may result in:

- Withdrawal of access to the Polytechnic's computing resources and/or network
- Legal or criminal proceedings

Singapore Polytechnic reserves the right to take legal action against an offending user in the event that he or she conducts himself or herself in any manner which is considered by the Polytechnic to be irresponsible; or in the event that the individual is misusing the computing resources allocated to him or her.

Visitor Acknowledgement

I hereby acknowledge that I have read the SP ICT Acceptable Use Policy for Visitors (this document) and that I understand its contents. I further acknowledge that I will strictly comply with the policy detailed in this guide.

I also agree to promptly and securely dispose any information or data obtained legitimately through the use of SP ICT resources, which are intellectual property or proprietary to SP, at the end of my engagement with SP or when they are no longer required, whichever is earlier.

Name: _____

Title: _____

Organization: _____

Phone: _____ (O) _____ (M)

Email: _____

Date: _____

Fill in the above PDF-fillable fields electronically (including email address) and email the completed form to the SP staff member, responsible for your visit/engagement. Ensure that you use the same email address to send the form, as this will serve as your acknowledgement.