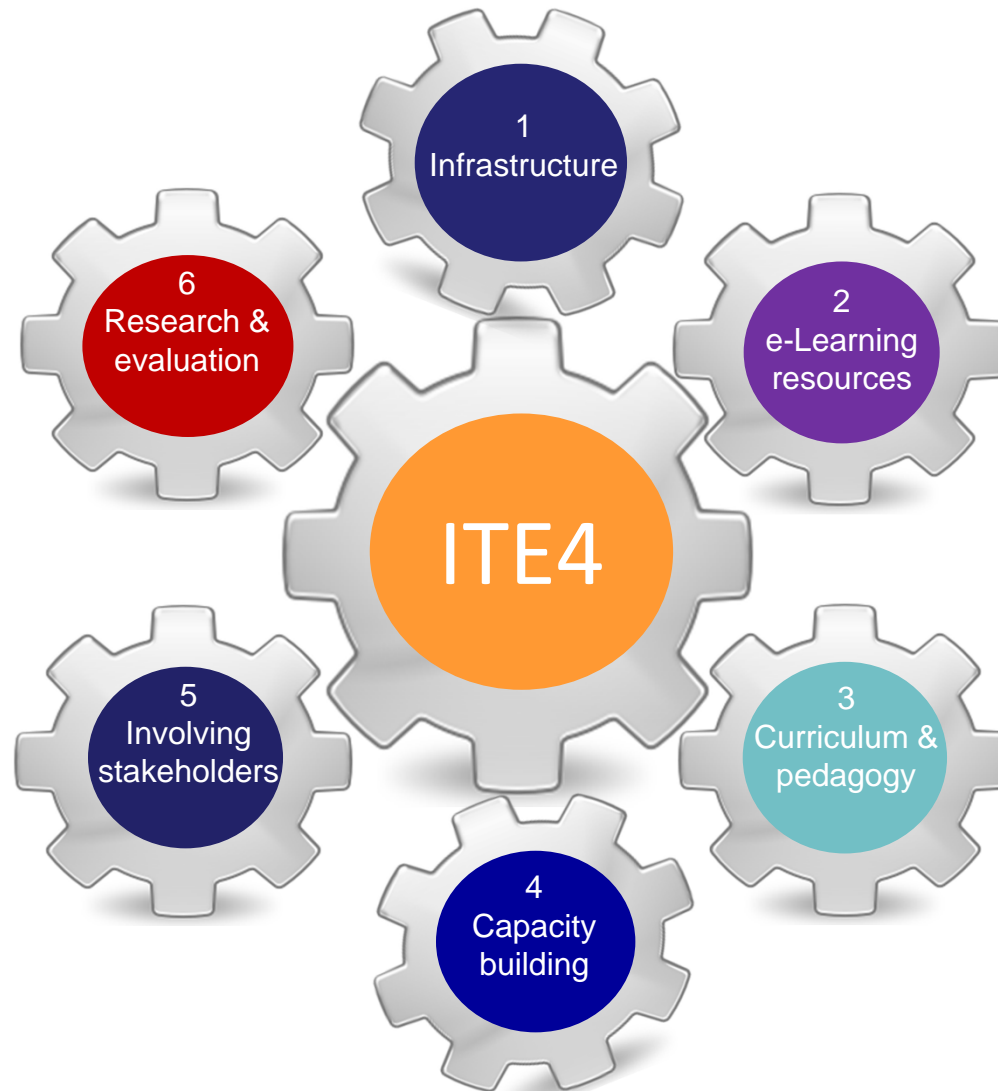


Information Security in Schools

**Sierra Lam
IT in Education Section
Education Bureau
28-29 Nov 2017**



Six Actions of ITE4



URL: <http://www.edb.gov.hk/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/ite4.html>



Development of ITE4

Relevance to information security

- Vendors
 - Infrastructure under WiFi100 and WiFi900
- Schools
 - Grants
- TSS / end users
 - Information Security in Schools – Recommended Practices
- Students
 - Information Literacy (IL) in curriculum

Infrastructure: WiFi100 & WiFi900

Terms and conditions in the specifications relevant to:

- Preventive measures
- Detective measures
- Responsive measures
- Recovery measures

Preventive measures

Design a secure network...

- Existing Network Facilities – not rely on any existing network facilities and cabling of the School, nor interfere with the existing WiFi network of the School. The Wi-Fi network shall be physically separated from the school network.
- The firewall policy should be applied to control network traffic such that public users should be prohibited to access the internal network segments of the School.

Preventive measures

Enforce Network Security Policy...

- The configuration settings of the appliance shall support blocking specific network ports, including ports of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Blocking denial of service (DoS) attacks and malformed packet attacks shall also be configured.

Preventive measures

Apply Access Control ...

- Authentication Method – use 802.1x standard based authentication and Hong Kong Education City single sign-on services.
- The WLAN system shall allow single or multiple devices per user account to be authenticated using 802.1x and Hong Kong Education City single sign-on service.
- The WLAN system shall suspend the session of the user once the session control is expired and the suspension time shall be configured by the school.

Detective measures

A proactive monitoring system is important...

- Managed Service – operate the WiFi network using managed service model, provide end-to-end service with single point of contact including configuration, provisioning of service, proactive monitoring, maintenance and regular reporting.

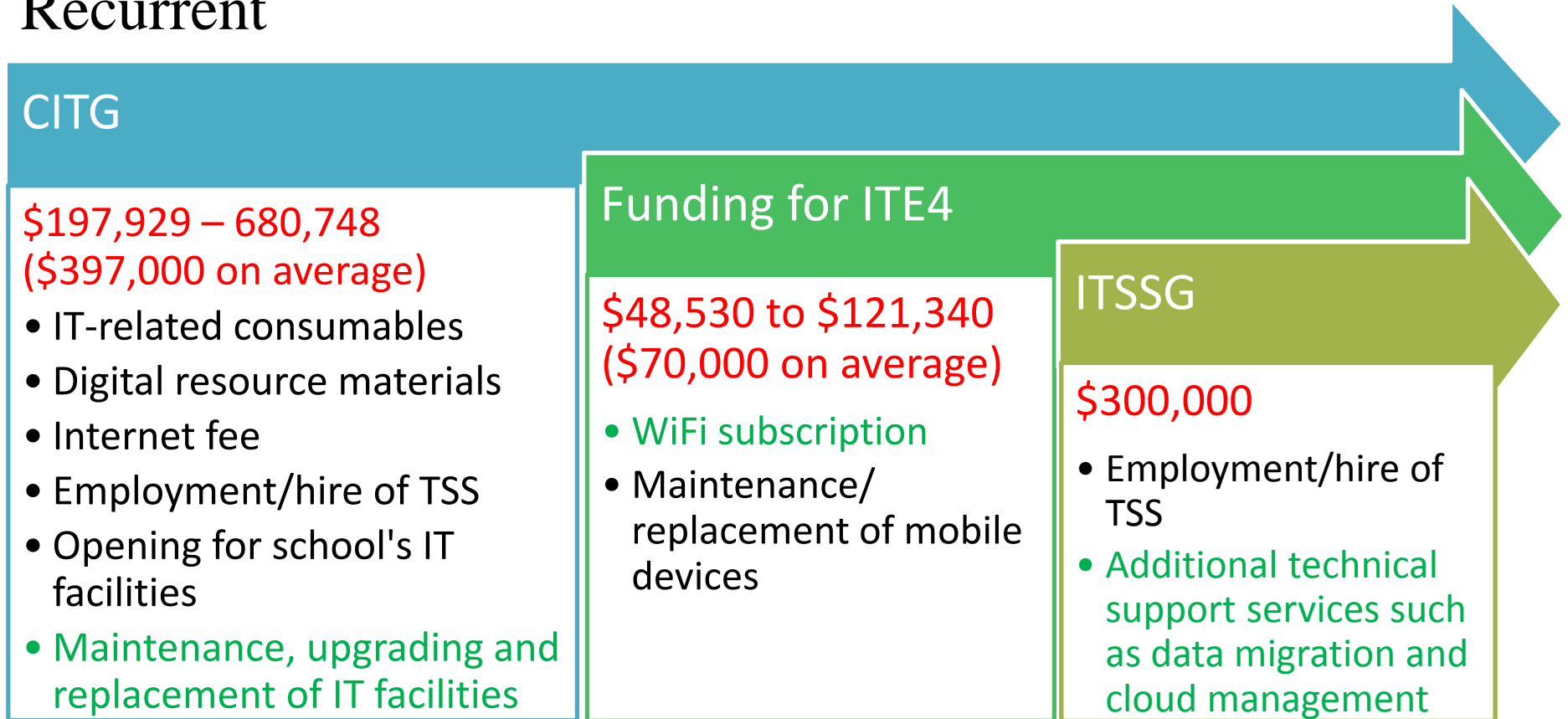
Responsive / Recovery measures

Define a response mechanism...

- Service Level Agreement – ensure at least 99.7% availability of the WiFi service, support four-hour response time and four-hour service recovery with active monitoring, helpdesk support with support hours from Mon to Sat 8:00 am to 6:00 pm, and provide monthly monitoring reports for the School.

Overview of ITE Grants

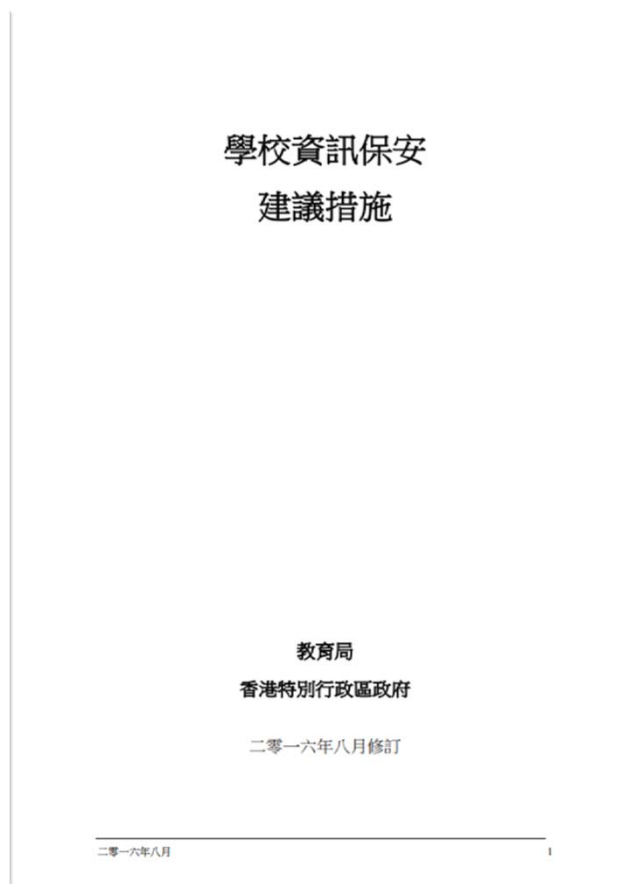
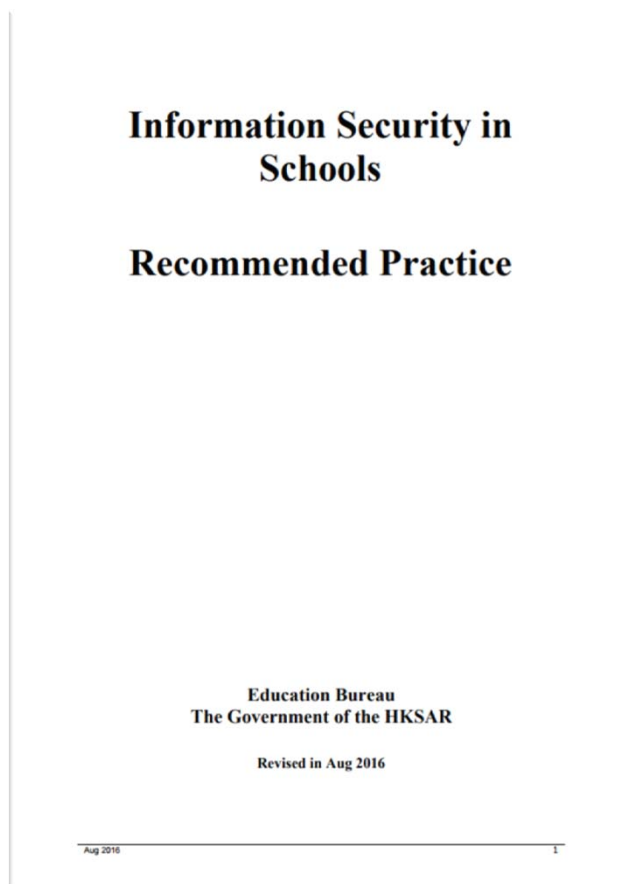
Recurrent



One-off

ITE4 (\$100,000) <ul style="list-style-type: none">• Mobile device	OITG (\$200,000) <ul style="list-style-type: none">• Mobile device• Employment/hire of additional TSS• E-resource/platform
---	--

Support for TSS / End Users: Information Security in Schools – Recommended Practice



Information Security in Schools

Security measures

- Preventive measures
- Detective measures
- Responsive measures
- Recovery measures



Image source: <http://thinkapps.com/blog/post-launch/adaptable-data-center-it-infrastructure/>

Suggestions to Schools

SECURITY INCIDENT HANDLING

Security Incident Handling

- Establish school-based IT Security Incident Response Team
- Setup proper reporting procedures:
 - Report to the school's IT Security Incident Response Team
 - School decision to report to
 - HKCERT? HKPF?

6. In addition to deploying security protection, schools should respond to incidents and invoke proper procedures in case an information security incident occurs. It is recommended that a checklist for security incident handling should be prepared. An sample checklist is given below for reference.

	Item	Details	Status
1	Establish an IT Security Incident Response Team	<ul style="list-style-type: none"> • Include IT Head, IT Technical Staff and other related staff; and • Publish the security incident response procedure to all personnel involved. 	
2	Escalation procedure	<ul style="list-style-type: none"> • All the security incidents should be addressed to the IT Security Incident Response Team upon such an incident is spotted. 	
3	Security incident response procedure	<ul style="list-style-type: none"> • Mitigate the effects caused by security incident; and • Protect the information resources from future unauthorised access, use or damage. 	
4	Reporting procedure	<ul style="list-style-type: none"> • Report on the incident and the ensuing investigation; • Summarizes findings regarding the Information Security Incident; and • Makes recommendations for improvement of related information security practices and controls. The Report will be distributed to the appropriate parties. 	
5	Training and education	Please refer to the following for detailed information in <ul style="list-style-type: none"> • Security Incident Handling for Individuals http://www.infosec.gov.hk/english/yourself/security_3.html • Security Incident Handling Guidelines http://www.ogcio.gov.hk/en/information_security/policy_and_guidelines/doc/g54_public.pdf 	

Information Security Website



The screenshot shows the Education Bureau website with a sidebar on the left containing links like Home, Latest News, About EDB, Press Release, Education System and Policy, Curriculum Development, Students and Parents Related, Teachers Related, School Administration and Management, Public and Administration Related, Access to Information, and Contact Us. The main content area features a banner for 'Information Security in Schools' with a date of (14/11/2017). The notice discusses ransomware attacks (Crysis/Dharma) and provides a list of preventive measures for schools, including blocking RDP access, restricting RDP use, applying the least privilege principle, using strong passwords, implementing account lockout, restricting IP access, and limiting remote connection time. A reference link to an HKCERT blog is provided.

Education Bureau
The Government of the Hong Kong Special Administrative Region

GOVHK 香港政府一站通 繁體版 簡體版 Mobile / Accessible Version My Colour A A Enter search keyword(s) Site Map

Home > Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education

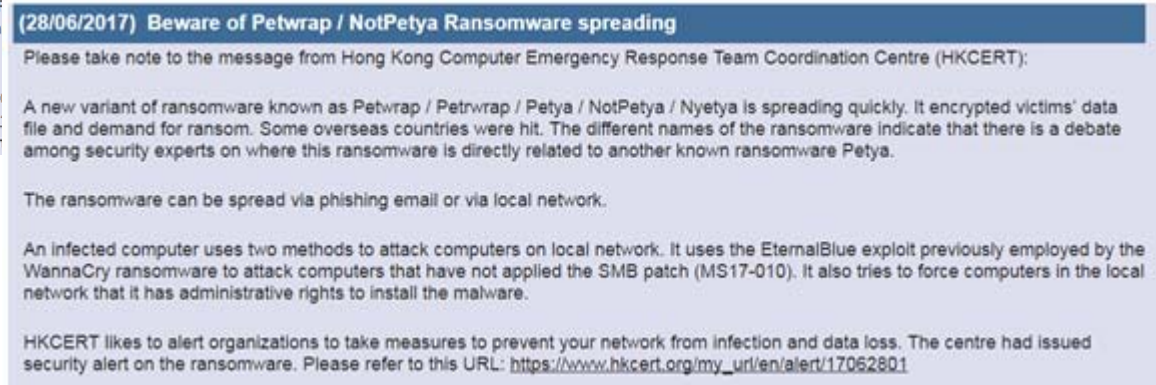
Information Security in Schools

(14/11/2017) Special Attention on Ransomware Attacks Leveraging Remote Desktop Services (RDP) for Infection

We notice that there have been reports of Crysis/Dharma ransomware attacks through RDP recently in Hong Kong, resulting in data being encrypted and inaccessible. TSS are advised to review and take the following preventive measures to protect the computers of your school from ransomware attacks:

- (a) Block RDP protocol access from the Internet. If remote access from the Internet is unavoidable, additional protection (such as VPN and multiple-factor authentication for the access) should be applied;
- (b) Restrict the use of RDP in computers;
- (c) Apply the least privilege principle to the account(s) that can remotely access the computer. Do not grant the administrator right unless necessary;
- (d) Use strong passwords and change password frequently;
- (e) Implement account lockout policy to lock out account after a set number of failed login attempts;
- (f) Restrict only specific IP(s) to access the RDP;
- (g) Limit the time period allowed for remote connection.

Reference:
Secure the Remote Desktop Services (RDP) for
https://www.hkcert.org/my_url/en/blog/1711090
Crysis/Dharma-variant .arena Ransomware Er



The screenshot shows an HKCERT alert dated (28/06/2017) titled 'Beware of Petwrap / NotPetya Ransomware spreading'. It advises organizations to take note of a message from the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT). The alert describes a new variant of ransomware known as Petwrap / Petwrap / Petya / NotPetya / Nyetya, which encrypts victims' data and demands ransom. It mentions that some overseas countries were hit and that there is a debate among security experts about its relation to other ransomware like Petya. The alert states that the ransomware can be spread via phishing email or via local network. It also mentions that an infected computer uses two methods to attack computers on a local network: it uses the EternalBlue exploit previously employed by the WannaCry ransomware to attack computers that have not applied the SMB patch (MS17-010), and it also tries to force computers in the local network that it has administrative rights to install the malware. Finally, it states that HKCERT likes to alert organizations to take measures to prevent their network from infection and data loss, and that the centre had issued a security alert on the ransomware, with a reference to the URL: https://www.hkcert.org/my_url/en/alert/17062801.

(28/06/2017) Beware of Petwrap / NotPetya Ransomware spreading

Please take note to the message from Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT):

A new variant of ransomware known as Petwrap / Petwrap / Petya / NotPetya / Nyetya is spreading quickly. It encrypted victims' data file and demand for ransom. Some overseas countries were hit. The different names of the ransomware indicate that there is a debate among security experts on where this ransomware is directly related to another known ransomware Petya.

The ransomware can be spread via phishing email or via local network.

An infected computer uses two methods to attack computers on local network. It uses the EternalBlue exploit previously employed by the WannaCry ransomware to attack computers that have not applied the SMB patch (MS17-010). It also tries to force computers in the local network that it has administrative rights to install the malware.

HKCERT likes to alert organizations to take measures to prevent your network from infection and data loss. The centre had issued security alert on the ransomware. Please refer to this URL: https://www.hkcert.org/my_url/en/alert/17062801

<http://www.edb.gov.hk/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/information-security.html>

Malware Prevention

Training and Education for End Users

- Avoid opening suspicious electronic messages, and do not follow URL links from un-trusted sources to avoid being re-directed to malicious websites
- Check attachments and downloads against malware before use
- Perform regularly data backup and keep them offline
- Prevent to use remote access software to connect to a school server or user workstation directly. Use secured channels (e.g. VPN gateway) with two-factor authentication for better protection.
- Use strong passwords and change password frequently

Handling Malware

Some of the ransomware infections and outbreaks in 2017 ...

Crysis/Dharma, Bad Rabbit, Petwrap / NotPetya, WannaCry ransomware attacks

In case a computer is infected, users should take the following **IMMEDIATE** actions.

- a) **DISCONNECT** the network cable of the computer to avoid affecting network drives and other computers;
- b) **POWER OFF** the computer to stop the ransomware encrypting more files;
- c) **JOT DOWN** what have been accessed (such as programs, files, emails and websites) before discovering the issue; and
- d) **REPORT** the case to relevant personnel/ organisation, such as ICT coordinator in school, HKCERT, HK Police Force, etc.

Information Literacy



The screenshot shows the Education Bureau website. The header includes the Education Bureau logo, the text 'The Government of the Hong Kong Special Administrative Region', and a 'HONG KONG' logo. Below the header is a navigation bar with links for 'GOVHK 香港政府一站通', '繁體版', '简体版', 'Mobile / Accessible Version', 'My Colour', 'AA', a search bar, 'Site Map', and an email icon. A left sidebar contains a list of links: Home, Latest News, About EDB, Press Release, Education System and Policy, Curriculum Development, Students and Parents Related, Teachers Related, School Administration and Management, Public and Administration Related, Access to Information, and Contact Us. The main content area features a banner image of children and a book. Below the banner is a breadcrumb trail: 'Home > Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education > Information Literacy for Hong Kong Students'. A 'Print' button is also visible. The main heading is 'Information Literacy for Hong Kong Students', followed by links for 'Introduction', 'Related Documents', 'On-going Support', and 'Related Links'. The 'Introduction' section contains two paragraphs of text about information technology and information literacy. At the bottom left, there are two small images: 'Insider's Perspectives' and 'Education for Non-Chinese'.

Education Bureau
The Government of the Hong Kong Special Administrative Region

GOVHK 香港政府一站通 繁體版 简体版 Mobile / Accessible Version My Colour AA Enter search keyword(s) Site Map

Home
Latest News
About EDB
Press Release
Education System and Policy
Curriculum Development
Students and Parents Related
Teachers Related
School Administration and Management
Public and Administration Related
Access to Information
Contact Us

Home > Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education > Information Literacy for Hong Kong Students

Information Literacy for Hong Kong Students

[Introduction](#) | [Related Documents](#) | [On-going Support](#) | [Related Links](#)

Introduction

Information technology (IT) is a powerful tool to unleash the learning capability of students. With the advancement of technology and its application through innovative pedagogies in all KLAS, students' capability in information literacy (IL), self-directed learning and other 21st century skills such as creativity, problem solving skills, collaboration skills and computational thinking skills are enhanced. Strategies on IT in Education are formulated at various stages to enable students to learn and excel through realising the potential of IT in enhancing interactive learning and teaching experiences.

As an important competency, IT helps students identify the need for information; locate, evaluate, extract, organise and present information; create new ideas; cope with the dynamics in our information world; use information ethically as well as refrain from immoral practices such as cyber bullying and infringing intellectual property rights. IL could be developed through the application of the generic skills (see Section 2.3.1 and Appendix 1 of this booklet) in the context of handling information in different media in our information world. This also involves various knowledge contexts and has close linkage with the KLAS.

Schools can make reference to the "Information Literacy for Hong Kong Students" for suggestions on how to develop students' knowledge, skills and attitudes to use information and information technology ethically and effectively as responsible citizens and lifelong learners. Incorporation of IL in the whole-school curriculum will provide authentic contexts for students to apply the skills and benefit their learning in relevant KLAS.

Insider's Perspectives
Education for Non-Chinese

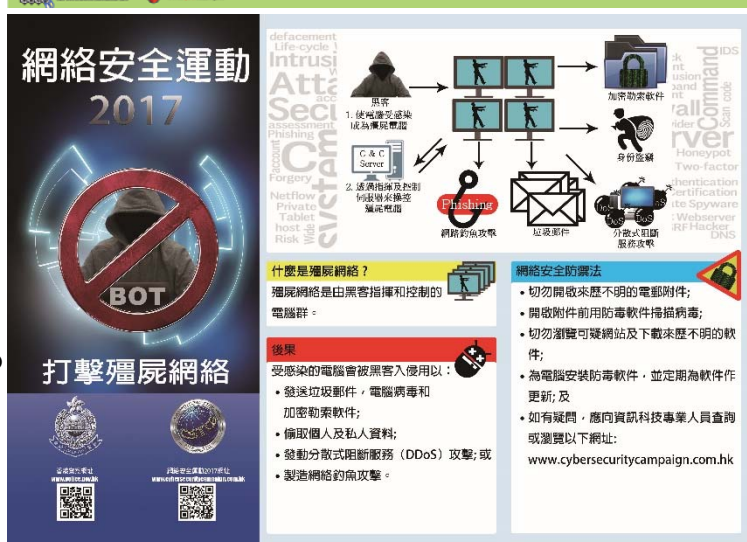
Source URL: <http://www.edb.gov.hk/il/eng>



Promotion of Infographics, Posters and Leaflets



<https://www.cybersecurity.hk/tc/resources.php>



<https://www.cybersecuritycampaign.com.hk/>



The Way Forward

Professional
Development
Programmes for Senior
Management and
Principal
IT coordinators /
IT team members

Migrate to Cloud
Services

Update the
“Information Security in
Schools –
Recommended
Practice”

What are the
needs of schools?
Any suggestions?



THANK YOU!

Enquiry

Use of Funds : (852) 3698 3606

Professional Development Programmes : (852) 3698 3610

Technical Advisory Services : (852) 3698 4148 / 3698 3566

