

# Principles and Guidelines for Internet usage at School

## Purpose

The purpose of this guideline is to ensure that

- a) Schools are informed about the applicability of principles and guidelines for Internet usage;
- b) Users of Internet are informed about the security risks of the Internet.

## Scope

The scope of the Guideline applies to all users in schools who have access to the Internet.

## Principles

The use of the internet is important in supporting high quality teaching and learning. It is expected that, in line with our aim to produce independent learners, the use of ICT and the internet are important tools, particularly in developing research skills and individualised learning programmes for students. This policy outlines the strategy to protect students and ensure a safe use of the internet.

## Guidelines/Rules for Students

Students will be made aware of the following rules when using the Internet:

- Only relevant information related to school work/ lessons should be downloaded.
- Students should never provide their contact details online.
- Chat rooms may not be used from within school unless as part of a prescribed piece of work, in which case the teacher will supervise the students. Students should be warned about the dangers of providing personal information and of even meeting the person with whom they have been chatting.
- Students should be discouraged from downloading freewares, music, songs games, screensavers and other unnecessary gimmicks since these may be infected with viruses.
- Beware of Phishing attacks. Phishing is the use of email messages and web pages that are replicas of existing sites to fool users into submitting personal, financial, or password data. Ensure you are on the right website with the right URL e.g. going to a web site for a bank whose real URL is <http://www.bankonline.com>. An attacker would probably send you an email telling you to go the bank's website at <http://www.bankOnline.com> which is not the real website but a copy of it from where all information you will provide thereon will be used to organise an attack against you.
- Do not surf on sites that contain offensive material.

## Using Email

- Beware of e-mails from unknown parties (unsolicited emails). Do not open unsolicited emails or respond to any unsolicited emails e.g. "You have won \$ 1,000,000. Kindly send your bank details for crediting your account."
- Executable files (e.g. with .exe, .com, .bat) and suspicious attachments should never be opened.
- Do not subscribe to unnecessary or unverified mailing lists. You may end up receiving an overload of emails that may slow down your computer. Such emails are known as spam.
- Regularly purge unnecessary emails (including emptying the 'Deleted Items' or 'Trash Can' folder) to free storage space.

## Student Protection

It is our intention to protect our students from inappropriate or undesirable material. The following criteria define inappropriate or undesirable materials:

- Obscene, offensive or inaccurate.
- Students must not insult, attack others, violate copyright, trespass in others' folders or harass anybody through the internet.

Under the **Computer Misuse or Cybercrime Act 2003** the Act provides for a repression of criminal activities perpetuated through computer systems. Attention is drawn to the following:

### **Indecent or Obscene photographs of children**

#### **Any person who –**

- a) takes or permits to be taken or to make, any indecent photograph or pseudo-photograph of a child;
- b) distributes or shows such indecent photograph or pseudo-photograph;
- c) has in his possession such indecent photograph or pseudo-photographs, with a view to it being distributed or shown by himself or any other person; or
- d) publishes or causes to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photograph or pseudo-photograph, or intends to do so,

**shall commit an offence.**

In addition, the school (including students, teachers and rectors) should never publish a photograph with the name of individual students. Where photographs are used in published materials in the school website, the school will ensure that:

- Parental permission is received.
- Photographs will be of groups of students with description such as "Members of Students' Environment Club".

## **Filters**

The lab network system is set up in accordance with best practices. At the Government Online Centre (GOC), our Internet Service Provider, we receive a filtered service. This filter screens out materials that are deemed as being unsuitable or undesirable. Students should not be allowed to use computers having dial-up access mode since they would bypass the filtering procedure.

## **Monitoring the Lab Network**

All teachers are expected to monitor the range of sites used. Ideally teachers should pre plan sites that will be used for downloading materials for classroom use. Periodically the teacher should undertake a routine check of sites visited and report any concerns to the Rector.

## **Supervision**

Albeit our aim is to develop independent learning within our students, it is agreed that total supervision at all times is not possible. It is therefore recommended that teachers regularly remind students of the responsible usage of the internet. Frequent checks by class teacher should be made while students are online.

During classes in the Computer Lab, the computers can be monitored by the staff present to ensure students are using appropriate web sites. Students should not be left in the computer lab unsupervised.

## **Reporting Student Misuse of the Internet**

In the first instance, the class teacher should deal with any misuse of the Internet directly with the child. Should there be concerns about the types of material accessed, the matter should be immediately reported to the Rector, who may contact the parents.

The sanctions imposed will reflect the severity of the incident and in serious cases, a student may be denied access to the Internet for a period of time.

## **Home Usage of the Internet/ Guidelines for Parents**

Students may have access to the Internet from their home computers. In these situations, it is incumbent upon parents to take personal responsibility for Internet usage at home. Rectors may advise parents to:

- Monitor their child's use of the Internet by placing the computer in a place that would be visible to them.
- Keep an eye on their child when he/she is surfing on the Internet.
- Monitor the time spent on the Internet.
- Take an internet package with filtering from their internet service provider (ISP).