وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

School e-Safety Policy Guideline

Version: 1.2

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: May 2018

Document History:

Version	Description	Date
1.0	Published V1.0 document	September 2014
1.1	Branding Change (ICT to MOTC)	May 2016
1.2	Format change + MoTC Logo changed	May 2018

Table of Contents

Legal Mandate(s)

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (22) of Emiri Decision No. 8 of 2016 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

This guideline has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Introduction

While the use of networked information resources can result in broad opportunities for educational purposes, the use of information and communication technologies (ICT) does not come without some risk of exposure to content and behaviour which may not be considered appropriate within the school or cultural setting of Qatar. This document is designed to serve as a foundation and framework for each school to develop appropriate policies and procedures related to the use of technology.

Naming convention has been defined as follows:

- **MUST/SHALL** the statement is an absolute requirement of the policy.
- **MUST NOT/SHALL NOT** the statement is an absolute prohibition of the policy.
- **RECOMMENDED/SHOULD** – use of this term indicates that there maybe valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT/NOT RECOMMENDED** – use of this term indicates that there maybe valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- **MAY** – the statement is a truly optional requirement of the policy.

Scope

The purpose of ICT use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions. Acceptable use polices related to ICT apply to staff and students and cover both school owned and personally owned equipment, such as the following:

- Computers and Laptops
- Networks
- Servers
- Webcams
- Digital video
- PDAs "Personal digital Assistance"
- Phones
- Portable media players

1 Internet Filtering

1.1 School Internet access **SHALL** be designed expressly for the use of students and **SHALL** include filtering appropriate to the age of students.

1.2 Internet access **SHALL** be planned to enrich and extend learning activities. Access levels **SHALL** be reviewed to reflect the curriculum requirements and age of students.

1.3 It is **RECOMMENDED** that an "allow-list"/whitelist be used to restrict access to a list of approved sites.

1.4 Administrators **SHALL** ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.5 Any material that the school believes is illegal **MUST** be reported to the appropriate agencies such as the Criminal Investigation Department 'CID'.

1.6 Schools **SHALL** maintain a current record of all staff and students who are granted access to the school's email and internet accounts.

2 Social Networking

2.1 Schools **SHALL** block/filter access to social networking sites, forums, chat rooms, etc. unless they are explicitly required for teaching.

2.2 Newsgroups **SHALL** be blocked unless they are explicitly required for teaching.

2.3 Teachers, staff, or administrators **SHALL NOT** run social network spaces for student use on a personal basis.

3 Intellectual Rights Policy

3.1 Schools **SHALL** ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.

4 Securing IT Resources

4.1 Policies and procedure **MUST** be established for account management, including creation, amendment, deletion and auditing of accounts. Accounts **MUST** only be created after appropriate acknowledgments by staff, students and parents.

4.2 Each staff member and student **MUST** have their own, unique, auditable account.

4.3 Users **MUST** take responsibility for their network use. For faculty and staff, flouting the Staff Acceptable Usage policy is regarded as a matter for dismissal.

4.4 System Administrators **MUST** set up system security.

4.5 Servers **MUST** be located securely and physical access restricted.

4.6 The server operating system **MUST** be secured and kept up to date.

4.7 Virus protection for the whole network **MUST** be installed and kept up to date.

4.8 The security of the school information systems **SHALL** be reviewed regularly.

4.9 Access by wireless devices **MUST** be proactively managed.

4.10 Portable media **MAY** not used without specific permission followed by a virus check.

4.11 Unapproved system utilities and executable files **SHALL NOT** be allowed in student work areas or attached to email.

4.12 Files held on the school's network **SHALL** be regularly checked.

4.13 The ICT coordinator/network manager **SHALL** review system capacity regularly.

5 Data Privacy

5.1 Personal data sent over the Internet **SHALL** be encrypted or otherwise secured.

5.2 Written permission from parents/guardians **SHALL** be obtained before images of students are electronically published.

5.3 Work can only be published with the permission of the student and parents/guardian.

6 Email Security

6.1 Staff or students **SHOULD NOT** consider their email private.

6.2 It is **RECOMMENDED** that email be restricted to approved addresses and filtered for unsuitable content and viruses.

6.3 It is **NOT RECOMMENDED** that email addresses overtly tie an individual to the email address.

6.4 Dummy email accounts **SHALL NOT** be used as one to one mapping is required for individual accountability.

6.5 Students **MAY** only use approved email accounts. It is **RECOMMENDED** that access in school to external personal email accounts be blocked.

6.6 It is **RECOMMENDED** that email sent to external organizations be written carefully and authorized before sending, in the same way that a letter written on school letterhead would be.

7 School Web Content

7.1 Staff or students' personal contact information **SHALL NOT** be published on any website.

7.2 It is **RECOMMENDED** that email addresses be published carefully, to avoid spam harvesting.

7.3 The school **SHALL** ensure that content is accurate and appropriate.

7.4 It is **RECOMMENDED** that the website comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

7.5 It is **RECOMMENDED** that any official blog or Wikipedia page associated with the school have access controls, be password protected and run from the school website.

8 Emerging Technologies

8.1 Emerging technologies **SHALL** be examined for educational benefit and a risk assessment **SHALL** be carried out before use in school is allowed.

8.2 Mobile phones SHALL NOT be used during lessons or formal school time. It is NOT **RECOMMENDED** that they be allowed in school.

8.3 The sending of abusive or inappropriate text messages is forbidden.

8.4 It is **RECOMMENDED** that the school evaluate wireless, infra-red and bluetooth communication technologies and decide on a policy for these technologies.

8.5 Staff **SHALL** be issued with a school phone where contact with students is required.

9 Incident Handling

9.1 If staff or students discover inappropriate sites, the URL **MUST** be reported to the IT Coordinator.

9.2 Internet issues SHALL be handled sensitively, and parents **SHALL** be advised accordingly.

9.3 Any criminal misuse **SHALL** be reported to CID.

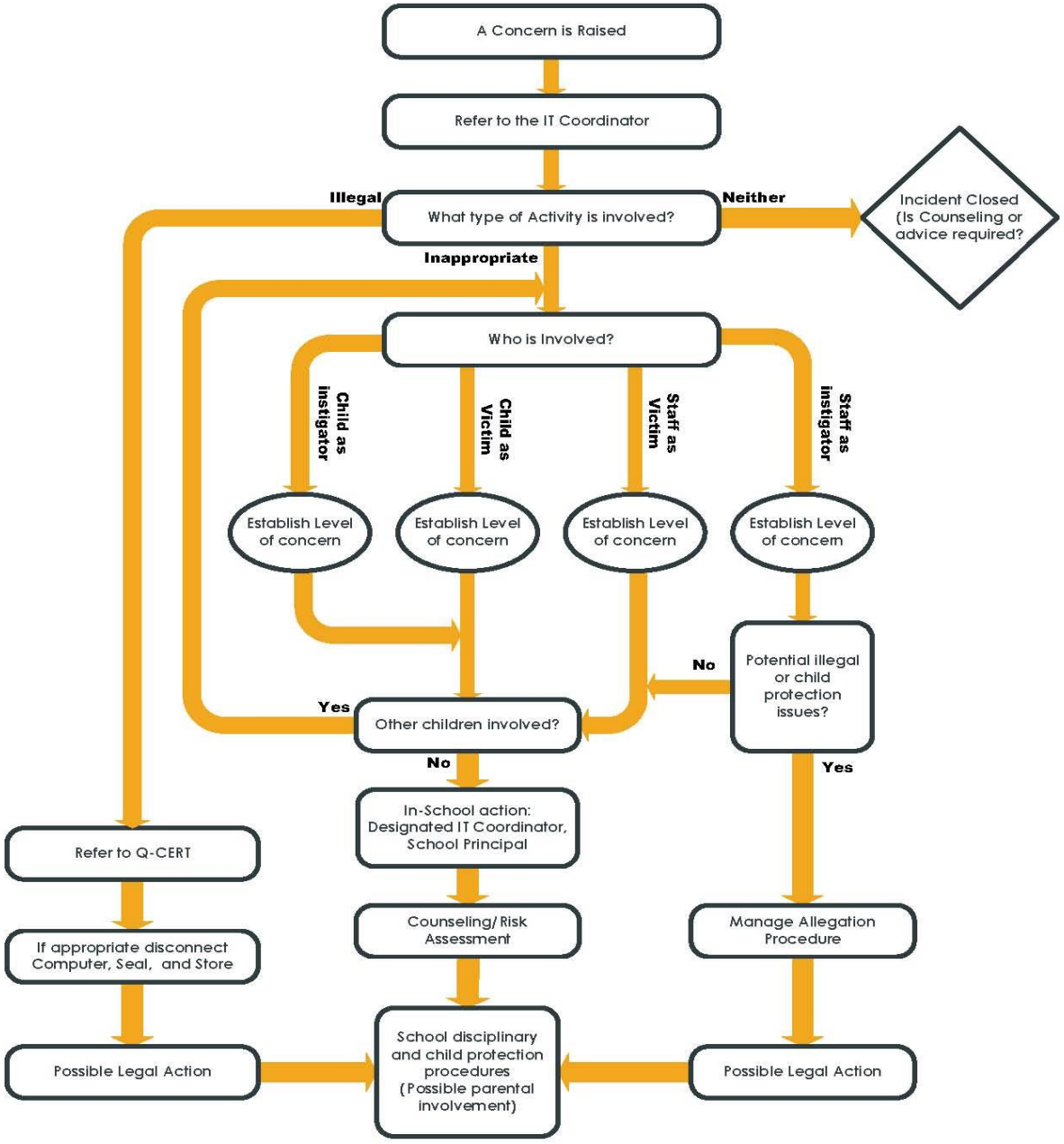

Figure 1: Incident Handling FlowChart

10 Auditing & Monitoring

10.1 It is **RECOMMENDED** that the school audit the ICT use to ensure if the e-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.

10.2 Methods to identify, assess and minimize risks **SHALL** be reviewed and updated regularly.

10.3 System logs **SHALL** be regularly reviewed to ensure this policy is being adhered to.

11 Awareness and Training

11.1 An e-safety training program **SHALL** be introduced to raise the awareness and importance of safe and responsible Internet use as well as the school's e-Safety Policy.

11.2 It is **RECOMMENDED** that instruction on responsible and safe use precede Internet access.

11.3 Student Acceptable Usage Policies **SHALL** be posted in all areas with Internet access.

11.4 Parents' attention **SHOULD** be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website. A partnership approach with parents **SHOULD** be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.

11.5 Students **SHALL** be informed that network and Internet use is monitored.

11.6 It is **RECOMMENDED** that staff be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

11.7 Staff that establish & maintain filtering policies or monitor ICT use **SHALL** be supervised by senior management and have clear procedures for reporting issues.

11.8 Staff, students and parents **SHALL** be informed that any criminal misuse will be reported to CID.

12 Disciplinary Action

12.1 The use of computer systems without permission or for inappropriate purposes **MAY** constitute criminal offence. Procedures **SHALL** be established to handle potentially illegal issues and how to report them to CID.

12.2 Complaints of Internet misuse **SHALL** be dealt with by a senior member of staff.

12.3 Any complaint about staff misuse **MUST** be referred to the head teacher.

12.4 Students and parents **SHALL** be informed of the complaints procedure.

12.5 Sanctions for online activities **SHOULD** mirror those that occur outside the online environment. Sanctions within the school discipline policy MAY include:

- Restitution
- Warning
- Reprimand
- Restriction
- Suspension
- Expulsion
- Interim or summary suspension

13 Roles, Responsibilities & Policy Management

13.1 All schools **SHALL** develop an e-Safety Policy based on this guideline document. It is **RECOMMENDED** that this policy restrict the use of personal ICT equipment in the school.

13.2 It is **RECOMMENDED** that schools have security policies covering their ICT equipment.

13.3 All staff **SHALL** receive and acknowledge the Staff Acceptable Usage Policy.

13.4 All students **SHALL** receive and acknowledge the Student Acceptable Usage Policy.

13.5 All schools **SHALL** review their e-Safety Policy at least annually.

13.6 It is **RECOMMENDED** that all schools appoint an e-Safety Coordinator that is responsible for the continued development and monitoring of ICT policies and practices within the school and in coordination with an approved board of governors.

APPENDIX A – AUDIT CHECKLIST

(*) denotes mandatory requirement

Policy Reference No.	Applicable		Complaint		Notes
	Yes	No	Yes	No	
1. Internet Filtering					
1.1*					
1.2*					
1.3					
1.4*					
1.5*					
1.6*					
Social Networking					
1.7*					
1.8*					
1.9*					
2. Intellectual Property					
2.1*					
3. Security IT Resources					
3.1*					
3.2*					
3.3*					
3.4*					
3.5*					
3.6*					
3.7*					
3.8*					
3.9*					
3.10					
3.11*					
3.12*					
3.13*					

4. Data Privacy					
4.1*					
4.2*					
4.3					
5. E-Mail Security					
5.1					
5.2					
5.3					
5.4					
5.5					
5.6					
6. School Web Content					
6.1*					
6.2					
6.3*					
6.4					
6.5					
7. Emerging Technology					
7.1*					
7.2*					
7.3					
7.4					
7.5*					
8. Incident Handling					
8.1*					
8.2*					
8.3*					
9. Auditing and Monitoring					
9.1					
9.2*					
9.3*					
10. Awareness and Training					
10.1*					
10.2					

10.3*					
10.4					
10.5*					
10.6					
10.7*					
10.8*					
11. Disciplinary Action					
11.1*					
11.2*					
11.3*					
11.4*					
11.5					
12. Roles, Responsibilities & Policy Management					
12.1*					
12.2					
12.3*					
12.4*					
12.5*					
12.6					

References

"Schools' e-Safety Policy Guidance, Kent County Council, April 2007." Becta | E-safety: the experience in English educational establishments