CCC EXHIBIT

Use of ICT facilities and devices guideline

This guideline supports the Use of ICT systems procedure that provides advice on appropriate and by implication, inappropriate use of the department's ICT facilities and devices when using the department's network and/or ICT resources.

Introduction and scope

Intranet, internet, email and other ICT facilities and devices are essential teaching, learning and business tools. ICT facilities and devices improve communications and workflow, enhance productivity and provide more flexibility for departmental employees seeking professional development opportunities and fulfilling their work responsibilities. For students, the department provides ICT access that enables the use of learning tools in support of the curriculum.

This guideline provides advice on appropriate and inappropriate use of the department's ICT facilities and devices.

This guideline applies to all staff and students using the department's network and/or ICT resources.

Network monitoring

The department monitors and reports on intranet, internet and network usage and inspects email messages sent or received by anyone using department's ICT business systems to:

- identify inappropriate use
- protect system security
- maintain system performance
- protect the rights and property of the department
- determine compliance with state and departmental policy.

If the department reasonably suspects you are using the network in a manner that could constitute a crime, the department will refer the matter to the police.

Monitoring and investigations include but are not limited to:

- accessing and examining specific types of messages, such as large messages or those containing documents, executables, audio visual files and/or compressed zip files
- accessing and examining messages in specific circumstances, such as at peak periods, where an individual's message volume is high, or on a random sampling basis
- accessing and examining records for the purpose of complying with investigation requests received from the Internal Audit Branch, senior management, or authorities such as the Queensland Crime and Misconduct Commission
- introducing and using content security software to protect users and the department's ICT network, systems and services from infectious or malicious content, offensive or libellous material and breaches of confidentiality
- conducting security audits and scans (whether manual or automated) of any personal ICT mobile devices that connect to the departmental network (whether used for departmental work purposes or not), where that device is used on departmental premises (e.g. school, regional office, central office) and/or is connected to the department's ICT network and a security breach has been detected or the device is suspected to have compromised the integrity of the network. See also the Use of mobile devices procedure.

CCC EXHIBIT

Use regarded as inappropriate

Inappropriate content and material must not be accessed, stored or transmitted on the department's network. The below provides specific examples of inappropriate use of the department's network including email, storage and internet access. This list is provided as guidance and is not considered an exhaustive list of inappropriate use. These actions by a user may constitute a crime under the *Criminal Code Act 1899* (Qld) or be viewed as serious misconduct under the Code of Conduct or the school's Responsible Behaviour Plan for Students.

Unlawful, criminal, offensive or obscene material

Uploading, downloading, storing, forwarding or in any way distributing or communicating the following:

- pornography
- inappropriate pictures, graphics, jokes or messages (particularly any material of sexually explicit, racist, sexist, discriminatory or otherwise potentially offensive behaviour, including the use of inflammatory, obscene, vulgar, insulting, abusive, threatening, harassing or provocative language)
- unlawful or criminal material
- any other material which is likely to cause offence or which would be considered socially unacceptable.

This includes the presence of the above information (whether accessed or not) on:

- external storage devices connected to the departmental network (personal or otherwise)
- personal mobile devices accessing or synching to the departmental network
- departmentally-owned mobile devices accessing or synching to the departmental network.

Defamatory and fraudulent material and use

- Uploading, downloading, storing, forwarding or in any way distributing or communicating information that is untrue, defamatory, libellous, misleading or deceptive
- Impersonating other people or falsely claiming to represent other people whether alive or dead, real or fictional
- Scanning images of another person's signature and storing or transmitting to other users – whether on purpose or by accident.

Use for personal profit or commercial purposes

- Using ICT facilities and devices to conduct personal business for personal gain or profit, including fee-based or subscription services or stock trading
- Uploading, forwarding or communicating any commercial advertising material or any commercial websites for personal gain.

Counterproductive use and exploitation of workplace resources

- Overseas or other expensive personal phone calls or IP calls (e.g. toll numbers)
- Downloading and/or playing any inappropriate or time-consuming games or software (e.g. Farmville on Facebook)
- Accessing gambling websites
- Accessing dating services online
- Accessing filesharing sites online
- Downloading or using filesharing software applications
- Downloading or storing files and records, including audio or video files in file sharing formats, which are not for officially approved purposes or that were obtained illegally, including using departmental resources to download to BYOx devices.

CCC EXHIBIT

- Downloading and/or distributing material such as chain letters or letters relating to pyramid schemes
- Knowingly performing any act which degrades or otherwise negatively impacts the performance of government ICT networks or an external party ICT network (e.g. downloading excessively large files or software, use of excessive amounts of bandwidth (e.g. audio or video streaming), spamming, transmitting files that may place an unnecessary burden on department resources or external parties
- Knowingly downloading and/or executing material from the internet, email or external storage device containing viruses, worms, Trojan horses, spyware or any other contaminating or destructive features
- Creating or maintaining personal websites (except in the course of authorised use of social media).

Political or religious advocacy

- Advocating religious or political opinions
- Participating in any lobbying or political activity or endorsing political parties or candidates.

Violating privacy and confidentiality

- Uploading or sharing personal information, including photographs or personal details (such as names, private addresses or telephone numbers) of third parties (including staff, teachers or students) without their prior consent
- Deliberately forwarding sensitive or confidential departmental information or documents to webmail or other personal email accounts.
- Intentionally scanning or photographing departmental documents or information and storing or circulating through un-approved channels.

Breaching intellectual property ownership

- Providing a third party information or material without obtaining the appropriate intellectual property permissions.

Contributing to public discussion in a way that is contrary to the public interest

- Using work email addresses when creating personal website accounts or profiles
- Making comments or disclosures concerning your official roles and duties (this includes disclosing work-related information, documents, images, etc.) or work-related activities and events unless the information is in the public domain
- Citing or referencing the department’s clients, partners, suppliers or employees without prior approval, except where such information is in the public domain
- Engaging in attacks or insults of any kind including:
  - online arguments or flame wars by participating in repeated hostile and insulting interactions with other users of websites or forums
  - trolling behaviour by posting inflammatory, extraneous or off-topic comments on websites or forums with the primary intent of provoking other users of the website
  - cyber-bulling, cyber-stalking or cyber-harassment by posting content with the intention to torment, threaten, intimidate, humiliate, embarrass or otherwise target other users of websites or forums.
- Engaging in any other action which could harm the goodwill or reputation of the department or the department.

Notification process for detection of inappropriate use

Where inappropriate use is discovered, the following steps must be taken:

1. Notify the Cyber Security team.
2. Director, Cyber Security and Identity Management to confirm with Director, ICT Sustainability that a policy breach has taken place.
3. Where information is illegal or illegally obtained, Cyber Security may delete the information upon detection.
4. Cyber Security to compile a report for noting for:
   a. Legal and Administrative Law Branch
   b. Integrity and Employee Relations
5. Report is passed to relevant director or school principal for disciplinary action. Where criminal activity has been detected, information will be passed to Queensland Police Service.

Limited personal use

Employees can use the departmental network for *limited* personal use.

The department permits occasional personal use of government ICT equipment and information resources, including computers, photocopiers, telephones, printers, facsimile machines, wireless devices, electronic mail and electronic services. Usage is monitored and recorded. Personal information e.g. financial details, can be inadvertently collected by the department's monitoring/investigation systems when the department's ICT resources are used for limited personal use.

Directors or principals can request information on employee network use at any time. This includes departmental mobile phone call and data use.

Scope of limited personal use for employees

Limited personal use is acceptable provided that such use:

- is infrequent and brief
- does not interfere with the operation of government
- does not violate any state/agency policy (e.g. Code of Conduct) or related state/Commonwealth legislation or regulation
- incurs only a negligible additional expense, if any, to the department
- does not impede or interfere with that employee's or any other employees' ability to do their jobs
- occurs during off-duty hours (off-duty hours are the periods of time when an employee is not expected to be working, such as during a lunch break or before or after scheduled work hours), whenever possible
- is not for the purpose of generating income for the employee or another individual (i.e. private business, personal gain or profit)
- is not in contravention to the above ‘Use regarded as inappropriate’ section.

Examples of limited personal use

The examples provided here assume that the employee is otherwise complying with the Code of Conduct, the Standard of Practice and, where appropriate, the specific rules of their school such as the Code of School Behaviour. Examples include but are not limited to:

- Using the telephone to:
  - make a brief call within the local phone area
  - make a brief long-distance call for which you then pay. (It is never permissible to charge personal long distance phone calls to the department.)
  - make alternative childcare arrangements if your child becomes ill

CCC EXHIBIT

  - notify your spouse or childcare provider that you will be working late
  - make or receive a brief call from family or friends.
- For acceptable use of a departmentally-funded mobile device refer to Use of mobile devices procedure. Generally, however, it is not acceptable to use a departmentally-funded mobile where a landline is available within reasonable proximity.
- Using internet and email facilities and devices to:
  - ask a co-worker/friend to join you for a social event
  - seek or provide advice regarding a recommendation for a doctor, tradesperson, etc.
  - briefly read news stories or other information of personal interest
  - contact your child's school to make arrangements for an appointment
  - send and receive brief emails from friends and relatives
  - briefly research items of personal interest
  - conduct a short personal online-banking session
  - check the weather forecast when there is a potential threat.
- Photocopying a short document or your resume.
- Using the printer to make a small number of copies of your resume.
- Faxing an emergency note to your child's school.
- Using the computer and printer to prepare a short letter or resume.

Security and licence

This document has an information security classification of Public.

Last review date: 31 July 2018 Ref: 16/380116