Submission to Crime and Corruption Commission

Operation Impala – An examination of corruption and corruption risks in relation to the improper access to and disclosure of confidential information in the public sector.

Queensland Teachers' Union

October 2019

QUEENSLAND TEACHERS' UNION OF EMPLOYEES EST 1889

1. Introduction

Established in 1889, the QTU has chalked up 130 years of achievement in professional, industrial and legal advice to the education and training sectors throughout Queensland. In 2019, the QTU is the voice of over 45,500 education and training professionals working in state schools, special schools, secondary schools, TAFE colleges, the dual sector entity Central Queensland University, and other educational facilities.

This QTU submission is made in the interests of our members, as well as the hundreds of thousands of students whom our members teach every year. While the QTU supports the privacy of students, their parents and our own members we believe that it is important that our members are made fully aware of their obligations in relation to the information they are entrusted with.

The Department of Education has been identified as an agency to be examined by Operation Impala with the focus of the investigation being to look at risks when employees improperly access or disclose confidential information. In summary, Operation Impala will directly target the use of Departmental computers systems and these systems are accessed by every school based Union member on a daily basis.

The OneSchool system is now ubiquitous in Queensland's schooling system and holds information on student management; curriculum and assessment management; finance and asset management; resource management and performance, reporting and analysis. OneSchool is used by members to meet their mandatory reporting obligations and is accessed by most members many times each working day.

In the recent past the QTU has seen charges laid against members previously for the improper use of OneSchool. A common feature of these files is that the member who is alleged to have committed the criminal offence had absolutely no idea that their actions were prohibited by the criminal code. In more recent times we have seen a member face criminal charges for accessing past exam papers stored on the school intranet for the purposes of assisting her daughter to study. Again she had no idea that her actions could constitute a criminal offence.

We have experienced numerous occasions when members have been unaware that it is an offence to access OneSchool to seek the address of a parent for a purpose not connected directly to their employment duties. Further, we find ourselves having to warn members not to use OneSchool to access information to help them answer Departmental disciplinary allegations due to the uncertainty around this issue.

OUT members have access to large amounts of confidential data but have been given little to no guidance by the Department in how this data can and cannot be used. The sources of control over Departmental data are not adequate to allow members to know what they can (and cannot) do with the information available to them.

These submissions will examine the current 'controls' exercised by the Department of Education as identified in the Operation Impala call for submissions.

We will also refer to the serious criminal charges our members are exposed to and make submissions on measures that can be taken to both protect and educate our members.

2. The current controls

The call for public submissions documents identifies a number of controls that the DoE exercises over the data held by the agency. These are contained in:

Education General Provisions Act 2006 **(the Act)**

Section 426 of the Act deals specifically with the handling of student, former student information in the possession of a public service employee (or former employee). The section states the person must not make a record of the information, use the information or disclose the information to anyone else, other than for a purpose of the Act; or:

- with the consent of the student or a student's parent;
- in compliance with lawful process requiring production of documents or giving of evidence before a court or tribunal.

Section 426 also states that information can be disclosed with the written consent of the chief executive, who may give the consent if he or she is reasonably satisfied the recording, use or disclosure is necessary to assist in averting a serious risk to the life, health or safety of a person, in the public interest; or necessary for specific types of research.

DoE Standard of Practice, February 2016

The standard of practice provides a broad prohibition on the sharing of privately information held on the Department's databases, as below:

> *'When using the department's computer systems, employees must not deliberately access, store or forward communication where doing so might result in a breach of the Copyright Act 1968 (Cth), the Ethics Act, the department's Information Standards and Guidelines or this Standard, or other legislative or policy instruments.'*[1]

The standard also reminds employees that, should they leave the employment of the Department, they have an obligation to maintain confidentiality of official information formerly available to them as a public official. [2]

Appropriate and ethical use of public resources

This policy refers to six principles in relation to the use of public resources. Relevant principles are:

- **Official purposes** - Resources must only be used for official purposes except where permitted for limited personal use.
- **Conflict of Interest -** An officer must not authorise expenditure that provides, or could be perceived to provide, a personal benefit to him/herself, or where there is a conflict of interest. The exception is where an officer approves (within delegation limits) expenditure from which the officer indirectly benefits (e.g. by improved accommodation or technology) or benefits as a minor part of a group (e.g. group professional development that the approving officer attends, along with multiple colleagues).

Information security

This 'policy' is a statement of the Department's intent to apply a '*consistent, risk-based approach to information security that maintains the confidentiality, integrity and availability of information by protecting information against unauthorised disclosure, access or use, loss or compromise (malicious or accidental), or a breach of privacy*.'

The document outlines the Department's idealised approach to the storage, use and security of information. There is little of practical value to Union members.

[1] P17 DoE Standard of Practice, February 2016
[2] P19 DoE Standard of Practice, February 2016

3. Criminal charges

If found to breach Section 426 of the Act a QTU member will have committed a criminal offence which carries a maximum penalty of 50 penalty points.

Section 408E (1) of the *Criminal Code Act 1899* (Qld) creates a simple offence for anyone who uses a restricted computer without the consent of the computer's controller with a maximum penalty of two years imprisonment.

Section 408E (2) of the CC increases the penalty to five years' imprisonment if the person accessing the computer causes or intends to cause detriment or damage, or gains or intends to gain a benefit. While Section 408E (3) increases the penalty again to 10 years imprisonment if the benefit gained is over $5,000, or the person accessing the computer intends to commit an indictable offence.

It is important to note that while the benefit gained can be a financial benefit, it does not have to monetary in value for the charge to be laid and the benefit does not have to be gained by the person accessing the computer themselves. It can be for the benefit of another person.

Relevantly, there is also a misconduct in public office charge, pursuant to section 92A of the *Criminal Code Act 1899* (Qld) that carries a maximum penalty of seven years' imprisonment.

We note that to access OneSchool, authorised users must first login and be authenticated by the Department's network. As part of the access, a two-factor authentication processes and various security measures and encryption protocols are employed. There is no doubt that the OneSchool system holds data can be considered confidential information for the purposes of Operation Impala and for the purposes of these criminal charges.

4. One School

The OneSchool system commenced its introduction to Queensland schools in 2008 and was used in every State School by 2013. Despite this, the Department has not yet released a clear policy, procedure or guideline which sets out in specific terms what the system can and cannot, be used for by members.

This has allowed a culture of liberal use of the OneSchool system as a 'one stop shop' for members when they need information contained on the system. For some members little thought seems to be given to the appropriateness of the accessing of information for purposes other than those directly related to their employment.

It is also the case that, until relatively recently there has been little interest on the part of the QPS in pursuing charges in relation to OneSchool access by teachers.

If Operation Impala is to increase the awareness of the need to improve security in relation to this information there is a very real risk of QTU members, who have acted with absolutely no criminal intent, facing serious custodial sentences because they were completely unaware that their conduct was prohibited.

The QTU asserts that the primary responsibility for ensuring their employees are fully aware of their legal obligations in relation to the use of OneSchool and other Departmental data systems must rest with government as the employer.

5. Submissions

The QTU urges the CCC to recommend that the Department of Education immediately create clear, practical and comprehensive policies, procedures and guidelines for teachers and school leaders that outline how the data they have currently have access to (and specifically data on OneSchool) can be used by them.

We submit that, while clear and practical guidelines for the entire public service on this issue is desirable, documents specific to the Department of Education are now essential. This not only because of the nature of the data that teachers and school leaders have access to but also because of the *Laissez-faire* culture that has been allowed to develop since the introduction of OneSchool.

Following the creation of these guidelines, extensive training should be provided to all State School teachers and school leaders by the Department of Education and this should be updated annually.

Finally, we submit that the CCC could recommend an 'amnesty' for Departmental employees who can credibly claim ignorance of the law in relation to the improper access to and disclosure of confidential information in the public sector, until the proposed training process has been completed.

While the QTU fully supports the intent of Operation Impala we are concerned that our members could become 'collateral damage' and submit that any recommendations in the ultimate CCC report to Parliament should reflect this concern.