CRIME AND CORRUPTION COMMISSION

TRANSCRIPT OF INVESTIGATIVE HEARING

CONDUCTED AT LEVEL 2, NORTH TOWER, 515 ST PAULS TERRACE, FORTITUDE VALLEY WITH RESPECT TO

File No: CO-19-1209

OPERATION IMPALA
HEARING NO: 19/0006

DAY 2 - TUESDAY 12 NOVEMBER 2019
(DURATION: 1HR 38MINS)

LEGEND

PO Presiding Officer – ALAN MACSPORRAN QC
CA Counsel Assisting – JULIE FOTHERINGHAM
HRO Hearing Room Orderly – KELLY ANDERSON
W Witness – TONY COOK
LR Legal Representative – N/A

HRO All stand.

PO Good morning, all. Ms FOTHERINGHAM.

CA Yes, good morning, Chair. I call the first witness, Tony COOK.

PO Mr COOK, do you prefer to take an oath or affirmation?

W I'll take an oath.

PO Thank you. I'll have you sworn in.

HRO You just need to take the Bible in your right hand and repeat after me, the evidence which I shall give.

W The evidence I shall give.

HRO In these proceedings.

W In these proceedings.

HRO Shall be the truth.

W Shall be the truth.

HRO The whole truth.

W The whole truth.

HRO And nothing but the truth.

W And nothing but the truth.

HRO So help me God.

W So help me God.

HRO Thank you. Take a seat.

CA Good morning, Mr COOK.

W Good morning.

CA You were given a Notice to appear today?

W That is correct.

CA Yes. May Mr COOK be shown the Attendance Notice.

W Thank you.

CA I tender that document.

PO Exhibit 25.

ADMITTED AND MARKED EXHIBIT 25.

CA Mr COOK, you are currently the Director-General of the Department of Education.

W That is correct.

CA And you commenced in that position in April of last year?

W That's correct. 2018.

CA And you had previously worked for six years in the Australian public service as the Associate Secretary for Schools and Youth within the Department of Education and training.

W That is correct.

CA And previously you have held several senior executive positions in the Victorian public service, including Deputy Secretary, Government and Corporate with the Department of Premier and Cabinet, the Deputy Secretary, Office for Children and Portfolio Coordination and Deputy Secretary, Office for Planning and Strategy and Coordination within the Department of Education Early Childhood Development.

W That is correct.

CA You began your career in Education Queensland.

W That's true.

CA And you are a registered primary school teacher with a Major in early childhood education.

W That is correct.

CA You have been Deputy Principal and taught in schools and preschools in Queensland and the United Kingdom.

W Correct.

CA And you hold a Bachelor of Education from the University of Technology.

W Queensland University of Technology, that is correct.

CA In October 2013 you were made the Honorary Fellow for the Australian Council for Education Leaders.

W Correct.

CA And you were awarded the Public Service Medal for outstanding public service, especially in driving schools' policy and funding reform in Australia.

W Correct.

CA And you were appointed to the Australian Institute for Teaching and School Leadership on the board on the 2nd of June 2015 and reappointed on the 14th of June 2018.

W That is correct.

CA Thank you. Has your agency prepared a submission? I believe it has.

W They have.

CA Yes.

W That is correct. Yes.

CA Thank you. I tender – no, sorry, that's already tendered. That's already part of the proceedings. What is your role as Director-General for your agency?

W So as Director-General my overall role is ensuring the effective running of the Department, including the appropriate delivery of educational services to approximately 550,000 students in State Schools in Queensland, as well as responsibility for early childhood education and regulation for early childhood education and care services, as well as responsibility for workplace health and safety and industrial relations more broadly across government.

CA Thank you. Would you like to make an opening statement?

W Yes, I do, if that's okay.

CA Please go ahead.

W Thank you. My name is Tony COOK, as mentioned I am the Director-General of the Queensland Department of Education and I have been in this role since April 2018. The Department delivers educational services to more than 550,000 students in 1,241 State Schools across Queensland. It is also responsible for administering the national quality framework in

Queensland and regulating early childhood services that are delivered by 2,983 providers to 305,320 children across the State. The Department also includes the Office of Industrial Relations which has responsibility for improving the health and safety of Queensland workplaces. To do all this the Department employs approximately 93,000 staff.

The Department welcomes Operation Impala and looks forward to how the findings can inform our practices in information management and information security. Given the focus of this investigation and the relative size and scope or our effort across the three portfolios that I mentioned I will focus my comments today predominantly on our approach to managing access to and use of confidential information in the schooling space. And I think my understanding is that the Office of Industrial Relations is actually not covered by this investigation.

Our core function is to support the learning and development of all children and young people in the early year years and throughout their schooling journey, equipping them for further success in their personal lives. Our commitment to embracing and supporting the unique talents and needs of all students is captured by our State School Strategy, a document that calls many contributors across our large dispersed multidisciplinary workforce to contribute towards our common moral purpose which is that every student succeeds. Everything we do as a system is aligned to this moral purpose and so to other systems and processes that support us to achieve this.

State School students come from a diverse background. They bring a range of unique abilities, experiences and challenges to their schooling. We know that understanding these factors and providing differential learning support relative to each student's personal needs is the better chance we have for preparing them for successful lives. Therefore, the collection and storage of personal information is a necessary function for educational systems. As school communities increasingly look to understand and support the specific needs of their students, the size, the richness and the sensitivity of our data grows. Practices that are undoubtedly to the benefit of students who need support, most for example complex case management, educational and curriculum adjustments and the reporting of student protection matters all require the collection, storage and sharing of personal data. We are custodians and active users of a range of sensitive personal information, including around the medical, behavioural, financial and legal matters of our students and our staff.

We make this data accessible to staff who require it in order to provide the best possible education for students. But we also have high expectations of those staff in upholding their legislative responsibilities around access and use of confidential information. We provide staff with policy advice and guidance through departmental publications such as our Information Security Policy, our Information Privacy and Right to Information Procedures, our Standard of Practice, which provides additional information to staff to support their understanding of the Public Sector Ethics Act and the Code of Conduct for the

Queensland Public Service.

The Department of Education is also signatory to the Youth Engagement Alliance Information Sharing Charter which provides detailed information about the handling and privacy of student data and what can and cannot be shared with other agencies, particularly for students at risk. This charter is a combined initiative of the Queensland Youth Engagement Alliance, which involves eight government agencies and three educational port folios. Teachers, guidance officers and principals and a range of other departmental staff hold trusted positions in our organisation and in the wider community.

Our risk appetite for the area of information privacy is low, with information security being one of the four enterprise risks we have identified in the Department's Enterprise Risk Management Framework and Policy. Breaches, even those driven by simple curiosity, are not tolerated. Our approach to information management requires a constant balance between two equally important factors. First we must ensure that data is accessible to the often broad range of people who need it to inform the service they provide to our students. We simply cannot provide students with the best educational opportunities if the teachers and other support staff who interact with them do not know enough about them to plan and provide targeted learning and support.

Secondly we must uphold our collective and individual responsibilities to access and use personal information only for authorised purposes. We constantly strive to achieve this balance through a culture that instils the expectation that information security is everyone's business, visibly championed by leaders and with an awareness of individual accountabilities at all levels of the organisation. By systems that support a Department-wide strategic approach to governance and the assessment and management of risks by protective measures to minimise risk of misuse, for example through access controls, user profiles, regular training, technological protections and deterrence and responsiveness to incidents and to constantly evolving nature of information security threats to strengthen our approach.

To support continuing improvement, information and security management these areas are a primary focus of our Audit regime, with 12 information management focussed audits conducted over the past five years that have particularly looked an our user access controls, information management, use of cloud services, security threats and vulnerability management, local administration rights and mobile device management. Since 2015/16 we've also assessed information management and security as a key component in 37 internal audits for various work units, processes and functions in our agencies, including correspondence handling, contract management, student protection controls and a range of central and regional office business units. These audits of the system, business unit and process levels provide us with the assurance about the effectiveness of our existing controls as well as evidence to inform our ongoing cultural, systematic and protective efforts.

For example, the policy and procedure to govern user access to OneSchool has been developed following a user access management internal audit report. This governance will reiterate the expectation of all employees to appropriately handle confidential and private information contained within the system. These reminders are already explicit on screen in that failure to take necessary precautions with information may result in criminal prosecution.

We acknowledge this is an area in which our work will never be done. A healthy information culture is not a project to complete but rather a life cycle that requires constant care and feeding. This is true both at the individual employee level and at the system level as we continually induct employees with comprehensive initial training to prepare them for their roles and make them aware of their accountabilities; to train staff to ensure they're capable of using the data sets for their work and aware of the need to ensure use is authorised and appropriate; to support and monitor through regular review of user access and staff interactions with personal data; to report any potential cases of misuse without fear of reprisal and to refresh regularly to ensure information security messages are relevant to changing circumstances and front of mind.

There are of course challenges to information management in a geographically dispersed multidisciplinary organisation that has approximately 93,000 staff. Technological advancements also pose new challenges as more information than ever is collected and is accessed. But for the most part technology allows us to mature in the quality of data-informed learning we provide to students and in the digital fingerprint that electronic data access leaves, serving as a deterrent to information misuse. It also has some pragmatic realities around prioritisation of our efforts in this space. While auditing and detection of misuse are a necessary part of information management there are costly and complex activities and we cannot afford to rely upon them alone as a deterrent to information misuse.

Just as in education we know the earlier intervention the better return on investment, in information security we see best value in growing and nurturing a strong information security culture, ensuring risk management is embedded in our systems and processes and acting a range of protective measures and responding promptly and fully into incidents and changing needs. Thank you.

CA Thank you Mr COOK for that comprehensive opening. And in addition to that, I will tender the submission.

PO Make that exhibit 26.

ADMITTED AND MARKED EXHIBIT 26.

CA You've already detailed your role in the agency, Mr COOK.

W That's correct.

CA I'll just show you the organisational chart for your agency. I tender that document.

PO Exhibit 27.

ADMITTED AND MARKED EXHIBIT 27.

CA Would you like to speak to that in any more detail by way of an overview of your department other than what you've already said in your opening statement?

W I guess my comments I'll make in terms of - I mentioned in Audits you'll notice that the head of internal audits reports directly to me as Director-General. It doesn't necessarily happen in all departments, but that's a deliberate strategy to ensure that I am regularly appraised of issues in relation to internal audits.

CA How often is that? Are there any set reviews?

W So we meet at least monthly, the internal auditor and I. I also meet twice a year with the Independent Chair of the Internal Audit Committee, so the Audit and Risk Committee. So I meet with that Chair twice a year. In relation to other matters in relation to particularly information security and information management you will see under the Corporate Services area we have particularly two areas I guess I'll refer to here. One is information and technology, and so we have a Chief Information Officer. So in terms of information security policy that policy work is driven particularly out of the information - the Chief Information Officer himself. In terms of issues around ethical behaviour and also issues around investigation under human resources area, and I understand you'll be speaking to Mr MILLER later today, our ethical area and behaviour investigations area is located in that human resources area, independent of where the policy advice might be driven in relation to information security, information management and policy as well. They're probably the three areas that I would raise to you in relation to the organisation chart.

CA Thank you. For Operation Impala the Commission is concerned with the educational side of things with the schools and the decentralisation. Can you describe the functions that your agency is responsible for performing in that area?

W In relation to school education?

CA And control and guidance over the schools, yes.

W So we have, as I mentioned earlier, we have 1,241 State Schools in Queensland. Those State Schools are divided across seven regional areas across the State. So we have seven regional offices. Within those seven regional offices we have each a Regional Director and then we have a number of other support staff, Assistant Regional Directors that work directly with schools to support schools in their function which is effectively the education of young people in our schools. We also have obviously the central office based in Brisbane, the central office's main role, as per the organisation structure, is through the development of policy and procedures but also some of those corporate functions in relation to matters such as payroll and the other matters that might be relevant obviously to an organisation the size that we've got. So we have about 88,000 school-based staff. Out of the 93,000 staff I mentioned earlier about 88,000 of them are school-based staff. About 53,000 of those are actually teaching staff in classrooms or teaching Principals or Principal staff.

CA And you mentioned that in general terms the type of private and personal information that your agency collects to perform its functions can include not only educational material, personal details of the children and their families-

W That is correct.

CA -and also in relation to - did you mention family law matters and domestic violence?

W I'm not sure I did at that time, but that's certainly information that was collected as well. So the first point of contact obviously for anyone entering into the schooling system is the enrolment form. And in the enrolment form we have a range of information that we do ask parents or care-givers or guardians in relation to information about not only their child but also themselves. And that enrolment form is a public form so it can be easily accessed by anyone in the public, it's available online. And that does collect information as you mentioned around areas such as personal addresses of students, but also their carers, contact information and phone numbers and email addresses, relationship status in relation to family, or carers, medical information about particular children, but also, yes, information about particular court orders that may exist as well is information we collect at that particular point in time.

Throughout schooling, then, there's a range of other information that we collect around obviously student performance information. So the performance of students, their report cards, there will also be information in there about student behaviour or any contacts that we make to parents or to carers or to guardians in relation to particular students, as well as any other additional information that might be relevant for a teacher or a member of staff to enter onto our OneSchool system, which is our system for collecting information in relation to students and families that will affect or may inform information about the education of that particular child.

CA But for the purpose of these hearings, the Commission is concerned with OneSchool as it is the main student database.

W That is correct.

CA Being a database where the public personal confidential information is stored.

W That is correct.

CA What do you see as the greatest risks and challenges in managing the privacy of the information on that database?

W As I mentioned earlier, one of our challenges of course is the fact that we have 550,000 students. We have a large organisation of 1,241 schools, as I mentioned over 50,000 teaching staff. We are also unlike other States, perhaps, much more decentralised in the State of Queensland, and so we have schools, for example, that are three kilometres from Papua New Guinea. We have one school that's spread over 17 islands and 48,000 square kilometres in the Torres Strait. We have schools that are far out west. We have many schools that are only one-teacher schools or teaching Principal schools. And so with that brings the challenges of school management and also the challenges of technology and ensuring that our network has the coverage in very rural and remote locations as well, to enable the effective access and use of OneSchool.

The other challenge that we have is the fact that the number of users or the number of daily interactions with the one-school software itself. So we have anywhere between 2.36 million users or user requests every single day, every single school day in relation to OneSchool. And that may be as simple as entering information about whether a child has attended school today or as complex of entering more detail about a court matter or court order that has been provided to the school today. So with that software where we have daily interactions of the nature of potentially over 3 million, it is the management of that, it is the understanding by teaching staff about the use of their data, but it's also the controls that we can put on that system without that system effectively grinding to a halt.

So we have to balance the security provisions, which we absolutely accept are vitally important for the information that we store in that database, but also with the usability of that database as well. So that's one of our challenges that we're always looking at. If there's changes that we're going to make to OneSchool system in relation to security, what is the impact of that change on the useability of the system to ensure that the system obviously doesn't struggle or it doesn't take 30 minutes for someone to enter information onto a system

The other bit for us is, as I mentioned in my opening statement, it is that

balance for the access of information. Because to some degree I would argue that our Department might be slightly different in the use of our information. The use of the information that we have available to our teachers is predominantly for the purposes of making a decision about a teaching program for a student. So a teacher does need to know information, for example, around a student's particular learning if they've got a particular diagnosed disability, and that information will go on to the OneSchool database. So teachers need to be able to access that information to then be able to actually ensure that they've developed an appropriate program or learning program for a particular student. The other one for us, of course you would imagine with a workforce of about 88,000 school-based staff, is the turnover. It's ensuring that we have regular training, regular induction for new staff, for ongoing staff. Where there are changes to policy and to legislation, we need to ensure that we update our staff and that we do that through our mandatory annual training that all staff are required to do. But also what other avenues do we have throughout the year to provide that training to staff that are predominantly school-based and actually in classrooms for the majority of their time.

CA Thank you. In relation to the risks for breaches of privacy for that confidential information, how regularly are those risks reviewed and mechanisms looked at for improvement in relation to systems, processes and people?

W There's two things particularly. There's probably more than two but I'll mention tow particularly. One is our enterprise risk framework. And so as I mentioned in my opening statement information management and the security of confidential and personal information is one of only four of our enterprise risks that we've identified. And again that framework is public. I'm happy to obviously, or table if you like me to, I've got it here.

CA Yes, could I see the table?

W Sure. So that's our Enterprise Risk Framework and you'll see in that framework the four areas that we have the lowest risk appetite for and one of those being the confidential and use of security of personal information. What we then do as a Department is every quarter our Executive Management Board, which is our highest decision-making board, that's chaired by me as the Director-General, it includes my Deputy Director-General and my Chief Financial Officer as well, and also a representative of one of my Regional Directors. So we receive a quarterly report in relation to our performance in relation to our enterprise risk management framework. And so we will have a report around information security particularly.

That report will include information about, perhaps, follow-ups in relation to particular audits and where we might be going around that. It will raise particular risks and risks that have occurred throughout the last quarter. It will provide information perhaps on where we might be going with renewing our training, our mandatory annual staff training program which includes a section

on info privacy and information risk and use of information. So that provides a report to the Senior Executive Board as the highest decision-making body of the Department.

Out of that we will talk about the findings of the risk report, and then make recommendations and accept the recommendations that might come out of that report for further work that might be need to be done. I also mentioned the internal audit regime. I won't repeat that again, but in my opening statement I talked about the fact we had a number of information security and information privacy specific audits around things like access controls, user profiles, use of the cloud. They're the sort of audits that have been focused on. As well as, then, in terms of other audits, for example, around I think we might do an audit on a particular regional office or we do audits on schools.

As part of those audits there's a category around information security and information privacy that the auditors will also examine. It will look at things like certainly user controls at a school level, but also things like are the necessary approvals in place at a school level that parents have given in relation to anything ranging from things like reproducing the image of a child, where parents have to actually give permission in relation to the use, then, of that information of a student's image in terms of a school's policy, and has the school followed those policies through. They're the range of things that happen as well.

CA Thank you. How often are these schools audits?

W My understanding is at least once every four years. That's my understanding. I would have to confirm that, but that's my understanding. And it's a rolling audit program across all of our schools. But I'm happy to confirm that. That's my understanding.

CA Do the schools themselves, if they're decentralised, do they, to the best of your knowledge, undertake their own internal audit?

W There's a possibility of a self-audit as in a self-reflection and self-assessment, but there's still a requirement for the internal audit team or the audit team to go in independently. The Queensland audit office also audits a number of our schools.

CA If that's every four years, I was thinking of something more frequent than a four-yearly review.

W For a self?

CA For a particular school.

W There's another area across from that as well which the school in – it's called a School Improvement Review, and so you've got the official audit which

looks at things like finances and things like that. A school improvement review looks at broader issues in relation to school performance around student learning outcomes. But a school at any time in relation to our information that we've got around procedures, a school at any time can self-assess, but there's no requirement for a school to self-assessment independently.

CA I tender the enterprise risk management framework. And if, Chair, you could read that into the record.

PO Thank you. I'll make that Exhibit 28.

ADMITTED AND MARKED EXHIBIT 28.

CA In relation to breaches of privacy that occur within your agency, what do you see as the impact on your agency's ability to perform its functions?

W So obviously breaches are significant when they do happen in our organisation, particularly in terms of the trust that we will have, particularly with families and the community more broadly. The community more broadly, but also certainly family members are aware of the range of information that we hold in trust because they provide that information to us. And so a breach of information from my perspective as the Director-General does impact on that trust. That then impacts on what we potentially are able to do to help particular families or help particular children because families, potentially, may feel that providing the information to us, if there's a breach of trust, may put their information at risk. And that's certainly something that we don't want as a Department. And so certainly you could argue it is a reputational risk. But more seriously for me it is potentially a risk in terms of a learning program for a student where we may not get all the information that we require to enable us to develop an appropriate learning program for that student if we haven't been able to show as a Department that the public can have confidence that their information they provide us is safe and won't be used for any purpose other than the one it is intended to be used.

CA Has your agency conducted any customer surveys of parents?

W So schools conduct surveys of parents. And that's provided in their school annual reports, the results in relation to that. I'm not aware of any survey that talk specifically about the treatment of information. It is about are you happy with the school? Are you comfortable with how the school operates? They're the sort of questions that are asked particularly of parents by schools.

CA And how would you describe the department's culture when it comes to misuse of information? How is the culture reinforced?

W Sure. So there's a few things in relation to that. First of all, I guess, in terms of an enterprise risk framework, the fact that we are public, but it's one of our

four enterprise risks that information security, misuse of information, ensuring appropriate management of information is included in our lowest risk at the time. And we do promulgate that. We do that in a number of ways: one is in relation to the mandatory annual staff training that all staff are required to undertake, including me, which has a range of modules. You're probably aware of those modules, or one of those modules is in relation to information security and protecting information. There's two aspects of that, there's the induction of that training, which is more detailed. And then there's the annual refresher that all staff are required to do which give scenarios. For example, it give you a school-based scenario and asks you questions about whether you think it's appropriate to share information in relation to a particular scenario. All staff are required to do that. It gets assessed and then they get a certification at the end of that.

CA Is that for information privacy?

W That's right.

CA And that's mandatory?

W That right, it's part of our mandatory-

CA Are they annual?

W That's right.

CA Are records of participation-

W -Yes, that's my understanding. And my understanding is that as of, I've got the number here, as of at the moment, 93,000, 88,000 staff have certainly done it. I don't know the breakdown of that in terms of school staff as opposed to all my other staff, I must admit..

CA Is it assessed?

W It is assessed online as you go. So if you get the question wrong it will tell you that you've got that question wrong. You can only get certified at the end of it and get a certificate of completion if you have successfully completed the program. It is an online program.

CA And does it contain specifically the range of disciplinary and criminal sanctions that can flow from misuse of information?

W So in terms of the material, it takes you through information around the information Privacy Act. It takes you through information in relation to our own Education Act. And so it outlines what those Acts include. I don't know the level of - it refers you to those Acts, but I don't know the level of information it has specifically around the sanctions. There are other places

where that happens; for example, in the OneSchool software.

CA Sorry, I just want to stay on this one at the moment and then we can talk about the software.

W Yes.

CA So yesterday we had a criminologist give evidence in relation to the deterrent effect of education, specifically concerning misuse of information, and Professor SMITH was of the view, backed up with his academic reading, that the training needed to include specifically to have a deterrent effect the entire range of sanctions, both disciplinary and criminal that could flow from misuse of information. So that would include a direct reference to the ability for a police referral by your agency, and that the charge would be under - the offence would be section 408E of the Code. If your training does not include that, particularly given the expert's evidence yesterday, would you consider that it would be a good idea to improve the deterrent effect of your training for that to be added?

W So we review our training every year. So based on what you've said to me, being more explicit around deterrents in both the training but also the other information that's provided to teachers, is something that we would certainly be willing to and open to look at for sure. So in terms of the in training I've just got it here in front of me, it talks about the Code of Conduct, it take you to what you should and shouldn't do. Based on the information I've got in front of me I can't find explicit – it takes references to legislation, so you'd have to go to the legislation and find, for example, in the Education Provisions Act it talks about I think it's 50 penalty points, and so it takes you through what the actually deterrent would be from the Act perspective.

CA But that's not the code?

W That's not the Code, that's right that's our own Act.

CA Yes.

W That is correct. In Education, of course, there's a number of deterrents that exist.

CA That would be the Education General Provisions Act Queensland 2006, Queensland section 426 about confidentiality?

W That would be the one, yes.

CA Yes. So that's not the same as the Criminal Code. That's a different one.

W No, it is not. I guess the only point I'm making is in terms of education, we've got a number of areas of legislation in which the use of personal and private

information is dealt with, including our own Act. But you're right in terms of the Criminal Code. The explicit to our employees about the consequences of misusing information, calling it out in the training would help all of our staff understand greater, I think, the implications of that.

CA See it could be confusing for them to just be told about section 426, as one of the operations of the Education General Provisions Act, and the elements of that are different from the Criminal Code.

W That's correct.

CA So section 426 talks about access and that there cannot be a record made or use or disclosed of the information, but there's an exception if it is directly associated with employment. I'll just go to that section.

So I think there's some confusion arisen with staff at your agency with section 426 and I'll go into that. So under section 426 it talks about (4)(a). It says, "The person must not make a record of the information, use the information or disclose the information to anyone else other than" and then part (b) says, "With the consent of the person." So it doesn't talk about the use having to be for directly work-related purposes.

W That is correct. In terms of that I've got it here in front of me. That's right.

CA Would you agree?

W With consent of the person to whom the information relates?

CA So if there's consent then there could be disclosure?

W That is correct, but I would-

CA For a work-related purpose?

W I would have to seek legal advice on that in terms of the interpretation of the Act. My view because this actually relates to the Education Act it talks about, you know, for the purposes of the Act, the purposes of the Act is for education. But I'd have to seek legal interpretation of how the Act is actually written.

CA It says subsection (4), "The person must not make a record of the information, use the information or disclose the information to anyone other than", and then it says, "(a) for the purpose of this Act, or with the consent of the person (b)."

W That's correct.

CA Anyway, that could be confusing, wouldn't you agree, when the entire range of penalty isn't – for the potential penalty sanctions aren't - your staff aren't

informed of the Criminal Code? I'll just bring up section 408E and show you a copy of it.

PO Exhibit 11, I think.

W Thank you.

CA You see with the Criminal Code, entitled computer hacking and misuse.

W Yes.

CA Includes it is an offence if it is unauthorised, namely not through the direct purposes of employment. And it is an offence for access only. And it is a circumstance for aggravation for a benefit to thereafter be derived. It doesn't talk about it being okay if there's the consent of the person to whom the record is being looked at. Do you see how the staff, wouldn't you agree, should be given the entire range of possible sanctions? They can see what might happen to them under the Education Act and then what might happen under the Criminal Code because they're two completely different offences?

W I understand the point you're making and in term of the range of legislation, I guess we particularly direct our staff, as you mentioned it is predominantly around our own Education Act, but also in relation to the Information Privacy Act as well. So as I sort of was mentioning earlier in terms of OneSchool, particularly if a teacher is generating a report, before they can actually print that report or save that report a message does comes up to warn teachers about the use of the data and the inappropriate use of the data. But at the moment our references in relation to that are our own Act, but also the Information Privacy Act. I think it would assist staff if we were more explicit at the point you're making, I think, around the Criminal Code. I think that would be beneficial to staff.

CA A good way forward.

W That's correct.

CA Thank you. I just wanted to go through while we're on this topic, some policies and procedures. Professor SMITH yesterday gave evidence that for a policy to be effective it needed to be viewed more than once. I'm taking it that if you have mandatory training that you draw your staff's attention to the policies at that time?

W That's correct. As well as anything that might be happening at a school level as well. So as you imagine with so many staff we have, particularly of the majority of those based in school, school principals have a responsibility as well about ensuring that their staff are aware of departmental policies.

CA And it needed to be consistent, so the policies, therefore, all of the schools,

however decentralised they are, need to adhere to.

W So there is one Department policy in relation to information security, and then there are procedures and guidelines behind that to take that policy and unpack that policy into some more practical and real life examples that we provide our staff. So effectively the central office establishes those policies. We would then provide communication out to schools about any changes to those policies, where to access those policies and then we provide the centralised training, the online training as well as additional training that we also provide on request in relation to information management security. We also have an I-Security website which is actually a public-facing website. You might be aware of that. Which is for parents and students and teachers, which also goes through the information around personal information, but also information security.

CA So for the schools do you provide them with prospective templates for their policies and procedures?

W The schools don't develop necessarily their own information police. They develop an ICT policy, and we so, we provide templates and examples of what they can actually provide in relation to that. But in terms of information security more broadly, is the Department policy and then the support documents under that so schools don't have to create their own policy in relation to information security. Their side of things in relation to ICT and misuse of data and things like that would be under their ICT school policy which includes things like use of mobile phones and use of personal devices in schools, and students actually have to sign an agreement with the school in relation to their own use of their own devices as well.

CA And Professor SMITH said that the policy should be simple, not too extensive or detailed and spell out the range of sanctions, the same as we were talking about with education. So I've just got a table of some of the policies and procedures that your agency provided to us in response to our questionnaire sent out for return in September. I'll just show you that.

W Thank you.

CA I tender that document.

PO Exhibit 29.

ADMITTED AND MARKED EXHIBIT 29.

CA So on the document we have seven different policies and procedures. So there's Access to Records Held in Schools Procedure; Information Privacy and Right to Information Procedure; Information Security Guideline; Information Security Policy; Information Security Procedure; Use of ICT Facilities and Devices Guideline; Use of ICT Systems Procedure. Wouldn't

you agree that for a staff member in a school that may be a bit confusing to try to get on top of all of those documents and draw out the relevant material? Would it be better for them to have some more simplified documents to look at?

W So just to explain I guess the hierarchy of the way that these materials exist. So the policy, the information security policy I guess is the head of our tree. And so that's a short, sharp few pages policy which provides basically the context of the importance of information security, the principles that we're based on, and then it goes through a range of definitions in relation to information security. To support policies within our procedures and under those procedures we talk about the roles and responsibilities. So what's the role and responsibility of a classroom teacher or an employee, what's the responsibilities of the Director-General, what's the responsibility of regional offices, what's the responsibility of principals. And so it does then distil that into much more detailed information to provide to staff.

Underneath that we'll then have a guideline, so a guideline is when we're actually getting to much more practical examples of what might happen. It might give some examples of things like a particular scenario, what should you do in this particular case? We do that deliberately. To put all that into one document I believe would create a document that's a large document. And so depending on the users of those documents we actually develop them in that particular way. It doesn't mean of course there can't be improvements. We always are looking to improvements, which is part of our reviews. But just to help the proceedings I was just – it would be useful to explain the hierarchy being the policy and then we do more detail and then we do more detail again. And for a classroom teacher I would argue the guidelines is probably what they would look at because it gives the practical real life example of a scenario that might happen in their classroom.

CA I've got a guideline here I'd like to go through with you. If we could just show Mr COOK use of ICT Facilities and Devices Guidelines? Just while we are gathering that together, how regularly does the Department review the policies and procedures?

W So under our policy framework policies to be reviewed at least once every five years; procedures at least once every three years. But there may be changes to legislation or changes to other matters which require those policies or procedures to to be updated more regularly than that. I think it is every five years. Let me check whether it is five or four. I do have that information for you in relation to policy. Yes, that's correct. So policy instruments are to be reviewed at least once every five years; procedures to be reviewed at least once every three years.

CA Do you think that it may be a good idea especially with the advances in technology for – and the risk associates with misuse for the public for your policies and procedures to be updated on a more regular basis than every five

and three years?

W We it depends I guess on the – we have a breadth of policies as you imagine. In this particular space, based on the table you just provided me, I think they have been updated every two years. I've got – most of them seem to have been updated twice over the last four years, is that that correct, in the table you just provided?

CA All of them have been updated twice in the last four years apart from one. The information security guideline has been updated once.

W Okay. So in that sense I guess in this particular space that the investigation is looking at that that has occurred and that might have been because of changes in legislation or the advance in technology. There might be other policies which aren't related to this particular topic which in fact the change may not occur until every four years or so.

CA So I've just got the use of ICT Facilities and Devices Guideline here which goes for five pages. The first part of it is of an deterrent effect that using – you state that using the network in a manner that could constitute a crime would lead to a police referral. That's halfway down the first page.

W Yes.

CA Which is good. But there isn't a definition for your staff – because you say this is a practical document the staff go to; is that correct.

W Guidelines generally are the practical document; that is correct.

CA There isn't a definition in here for unauthorised misuse of confidential information. Page 2 talks about what is regarded as, and it is termed "Inappropriate", and there's some examples given there which go for two pages. But nowhere in the document does it define unauthorised use. The nearest I can see to that is on page 3, which talks about violating privacy and confidentiality, and under there it says, "Uploading or sharing personal information" and gives some examples 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. Is that derived from section 426 of the Education Act?

W Sorry, which section in particular?

CA Halfway down page 3, under the subheading “Violating privacy and confidentiality.”

W Yes.

CA It says one of the inappropriate acts is to upload or share personal information

of third parties without their prior consent. The inference being there that if there's consent that can be done.

W I cannot answer that question. I mean, I didn't write this particular document. So I can't answer in terms of whether it actually was derived particularly out of the Education Act or not.

CA Would you consider that now we've had a discussion about section 408E and the need for your staff for the deterrent effect to understand and be aware of that section of the Criminal Code and the eminence of it, that unauthorised use be defined within this document and their attention drawn to section 408E?

W I think anything we can do to improve the information to our staff, including as you indicated as a reference to the Criminal Code Act here, but in fact we haven't gone further and been explicit around that. So-

CA There's no – I can't see a reference to the Code. On the first page it says, "If the Department reasonably suspects you are using the network in a manner that could constitute a crime, the Department will refer to the matter to the police." Then I can't see anywhere in the document that it mentions the Criminal Code or section 408E.

W So on page 2 up the top, "These actions by a user may constitute a crime under the Criminal Code Act 1899" and there's a direct link to the code itself.

CA Right. Yes.

W So that's my reference there, but I think as a department we can go further in terms of providing support to our staff. Links are links, whether people actually then follow that link is a question and being more explicit around that I think would be a useful improvement to our material.

CA That's the direct link to 408E.

W Yes, I don't know whether that link links directly to that or whether it's – I'm assuming it would just be the code but I don't know. But I think as you've mentioned, anything we can do to be more explicit about that section would only be helpful for our staff.

CA Thank you. And the teachers union have provided a submission and there's a representative going to appear – I tender that document.

PO Exhibit 30, thank you.

ADMITTED AND MARKED EXHIBIT 30.

CA The teachers union have provided a submission. Are you aware of that?

W I'm aware of that, that's so.

CA Have you read that document?

W Yes, I have.

CA Would you like to be provided with that document whilst we talk about it?

W That would be useful. Thank you. Thank you.

CA So on page 4, paragraph 7.

W Under OneSchool?

CA Yes, you mentioned OneSchool before and that's the main database that we talked about. They say in here the teachers union how it commenced in 2008, so that's 11, almost 12 years ago now, and is due to be in every school and was used in every school by 2013. So that was a while ago as well. And they say that 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 staff. What do you say about that?

W So there's a few things around that. In relation to the actual OneSchool there's obviously user guides in relation to OneSchool, there's a OneSchool level access guide. There's work – we are developing a new OneSchool access management policy and procedure for next year which actually looks at user access and user profiles and the review of those quarterly. In terms of OneSchool itself, when a teacher logs on to OneSchool they do get a particular statement in relation to the use of data in relation to OneSchool. So they get two sources of information. They get information about the responsible user agreement, which actually to logon they have to click and acknowledge that agreement before they can enter into OneSchool.

CA What's the contents of that agreement.

W I'm happy to table this as well if that's useful. This is the screenshot of what actually comes up.

CA Is it something that we are able to have as part of the evidence?

W My understanding is it would be. I don't see any issue why it wouldn't be. It just talks about, you know, what's the OneSchool's – what it's use or access, so understanding access is through a particular PIN and that your PIN should not be shared with other people etc etc. That you will do things like collect information that you might have printed out from the application immediately rather than leave it on the photocopier. So it's actually about the treatment of that data. Your professional duty of care in relation to misuse of the information and that it may be an infringement of the Department's code

conduct and that you understand and agree to the conditions and you abide by those conditions as any other conditions that might be imposed by your school. And so a teacher then, or a person accessing that, then clicks that as an agreement in relation to entering the OneSchool system.

CA Can I just have a look at that document?

W Sure.

CA Professor SMITH talked about warnings for the log ons yesterday and the same recommendation as education and policy that there should be reference made there to the potential for the criminal sanction.

W Certainly.

CA So having had this discussion today, would you also think that would be a way forward to amend your warning agreement to include that?

W So, yes, so we then have a second warning agreement which in relation to then actually generating reports. It has references to two forms of legislation, but it doesn't have reference to the Criminal Code. And so that's an improvement that we could look at in relation to that particular warning that comes up to staff when they generate a report out of a school, which they may save or they may print or whatever it may be.

CA Is this the warning that you have just given me, the agreement, is that to obtain access?

W That is to actually get in. So every time you start up OneSchool, my understanding is that like – like for me when I start up my computer at work I also get a agreement effectively that I am making to get into the Department network and that agreement talks about Code of Conduct, our standard of practice, the Public Sector Ethics Act. It talks about misuse of the data. So that's what comes up for all employees to start with. And then beyond that you've got the OneSchool access, which is what you got then to start up OneSchool, that would come up and a teacher would click an agreement to that to that enter into the OneSchool system.

CA Wouldn't you agree that the reference to the disciplinary and criminal sanction should be on this given that an offence under section 408E of the Code includes access?

W I think I've agreed to that. I think I've said that I think being more explicit to staff around the implications of the Criminal Code is something that as a department we should look into which includes the second I guess agreement effectively that a teacher is making in relation to, as I mentioned, when you actually generate a report out of OneSchool, there's a second screen that appears before you can actually save or print that report. That report talks

about responsibility to keep the information safe, and it talks about failure to take these precautions may result in criminal prosecution. And then it talks about this, the Education General Provisions Act and civil penalties for the Information Privacy Act. I think we can strengthen that by referencing the Criminal Code as well. It talks about, you know, you must ensure you have lawful authority to provide to – to generate this information, but also to provide this information to other people. So we can look at that. I think we should look at that warning to see what we can do to strengthen that warning.

CA For completeness, are we able to have that as well to go with this?

W Sure.

CA Yes.

W The third one unfortunately I don't have a copy of, but the third one, as I said, was the general agreement that anyone makes when they enter into our Department network. I've got a copy like this, but I don't have a copy to hand to you. But we can provide that if the Commission does require that as well.

CA I tender those documents.

PO Exhibit 31.

ADMITTED AND MARKED EXHIBIT 31.

CA And then the teachers union at the bottom of that page 4, urge for the outcomes of Operation Impala to lead to your agency immediately creating clear practical 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. And you've undertaken to take on board-

W We're very happy for feedback such as that. And as you would expect, we meet – I meet with the Queensland Teachers Union with the executive at least once a month to talk about particular issues. This issue hasn't been raised in the time that I've been here as a particular issue that's been raised in those meetings, but notwithstanding anything that we can do to make information – to make our staff more aware of their responsibilities, as I've indicated and as you've provided in the evidence there are a range of policies and procedures that we have. Add to that the mandatory annual staff training, which requires teachers to actually make decisions and be assessed on those decisions about the use of data. But anything that we can do to improve that is something that as the Director-General I'm always open to.

CA Thank you. I'll just touch on, you've already gone into a lot of detail in your opening statement about access controls and auditing, but I just want to run through a couple of things. So just to clarify, it is password restricted for

OneSchool? Each user as has to-

W That's right.

CA Yes.

W Has a PIN, that's right.

CA And how do your supervisors monitor staff that they don't share passwords?

W Monitor? I'm not sure there's a monitoring. It's the training and the preventative side of things. I'm not aware of the monitoring in relation to sharing of passwords. I'm certainly aware of again the information that we provide to staff that they are to actually not share their passwords. Again, that sort of comes up on those screens that I provided you with earlier in relation to that matter.

CA And there's an audit log for OneSchool?

W There is. Every time someone accesses OneSchool that is logged. And they can do that from home as well as through the – if they access it from home on their home computer that is still logged.

CA And are all staff made aware of that function as UI?

W I must admit I don't know the answer to that question. I can find out, but I'm not aware of that. I'm not aware of the answer to that particular question.

CA If they aren't would you consider including that in any updates to your policies and procedures and educational material?

W Absolutely. Unfortunately I've given away to you my screen. I'm not sure whether it actually says that on the actual – sorry about that. So it talks about them agreeing they won't share their log in their PIN to another person. The general entry point does indicate that the ICT – the use of the network including the user of the Internet and emails monitored by information and technology branch and any wrongdoing can be traced. Information you enter, access and store on the Department's network can be accessed by the Department as well. So the first point of entry into our system does provide information about the fact that what you put in is being monitored or your access is being monitored but we're not explicit based on this information that I've got in our entry screen to OneSchool about logging your entry. And that's something we could look into in terms of improving that as well.

CA And with your access controls are they able to be to be individually assigned in accordance with roles?

W That's correct. We have user profiles.

CA And how do you as a Department provide guidance to the decentralised school base that you've spoken about?

W So we have those documents that I referred to just minutes ago. So there's actually a user access guide. Just get the correct name for it. The OneSchool Level Access Guide is information that's provided to schools in relation to that particular matter.

CA Yes. And we've talked about auditing. That's once every four years.

W So that's for schools.

CA Yes.

W But we have an internal audit regime which has an annual audit program. And so the ones that I mentioned earlier in relation to the 12 that were focused particularly on information security over the last four years or so that's independent of school audits.

CA And you haven't got data analytics at all?

W About? About?

CA So being able to do proactive detection.

W So in our system at the moment it still is really effectively manual logging in the sense of we actually do get printouts and we check about unusual activity.

CA Yes.

W But in terms of the actual IT systems about flagging, no, in our system, currently it is limited in relation to that.

CA How often do the reports in relation to access logs, how often are they reviewed and what sort of activity do you look for as unusual?

W I'm not sure I can answer that question. I would need my CIO to do that.

CA Yes, if you're unable to, then if you could let me know who can?

W The Chief Information Officer in relation to – would be able to assist in relation to that matter.

PO Mr COOK, do I understand correctly that currently is a manual process, the printing out of the log activity?

W That is correct. That is correct.

CA Are you able to – for some of these questions I understand you may not be able to and there's other people who can address that-

W Sure.

CA Once there is a detection of potentially an unusual access, do you know the process from that potential breach being assessed and then actioned if there's – who does it and how long it takes for that process?

W I think Mr MILLER might be able to help you a little bit more about that-

CA That's fine.

W -because particularly if it is an issue that we believe – it can start off at a school level. So, again, for the majority of our staff being in school, that was something that would be drawn to the attention of the school principal. The school principal then making decisions about the nature of that particular issue and then whether in fact that has to go further in terms of ethical investigations branch.

CA And in relation to you mentioned that some of the more sensitive information you hold relates to people's health; any families going through the family law process; and domestic violence matters. For a vulnerable person of the public such as a domestic violence victim, you say that they provide you with copies of their orders.

W Potentially, yes. So we have an ability to have a court order recorded. Whether it's a copy of it – well it would be a copy of it at the school level, that's correct, yes.

CA And at times some of those victims of domestic violence may be concealing their location and contact details from their former partner. What protections do you have in place by way of instruction to your staff and access to that particular record where you know, say, for example, there's a domestic violence order on there, where, say, the ex-partner telephones the school, which they can do, if obviously they've got children together and they manage to obtain the details of the domestic violence victim who doesn't want their address shared with their ex-partner. How do you prevent that from happening?

W Yes, so in relation to the OneSchool software we have a section around court orders and so that would be flagged effectively in the OneSchool record.

CA How do you flag that?

W Well there's a section off to the side. Sorry I haven't got a visual for you, but there's a section off to the side when you bring up the student's name that talks

about various categories and the section that may talk about court orders will be ticked so that the staff member would know there's a particular court order in relation to that particular student or the mother or the father or the caregiver. Do we – have we got a system where we then suppress that information? That's a system we don't have that currently. So we don't have – we don't have – I did see some of the evidence yesterday I think of TMR where they might have something where, you know, only certain users could access that information. We don't have that. Short of the user profile in relation to a school and the teacher and the principal in that school, we don't have a system at the moment that automatically redacts, if I use that word, particular issues around domestic violence.

CA If the ex-partner telephones, is there any record made if the domestic violence victim have let the school know-

W Yes.

CA -"my details are confidential"?

W Yes.

CA Is there anything put on the system so that then whoever – staff member accesses OneSchool they can see that and then not provide the details.

W That is my understanding. I don't use OneSchool myself. In fact I checked this morning and my access has been revoked because I haven't used it recently. And I shouldn't be using OneSchool because there's no reason for me to get into individual scenarios about individual children as the Director-General. But I am aware because of the information that comes to me effectively every interaction between the school and a caregiver or a parent is effectively as much as possible actually recorded on OneSchool. And so certainly information where someone has specifically requested non-disclosure of information would be recorded on OneSchool.

CA And I will just go into governance. In the Department's submission on page 1, paragraphs 1 and 5, you talk about good governance and being committed to that. Other than what you've said in your opening statement, is there anything else that you would like to speak to in relation to governance, in particular, ethics, code of conduct, strategic plan, integrity framework? You've already talked about some of that.

W Yes, and I won't repeat that short of I guess what I mentioned earlier. From the most significant decision making body of the Department, which is the executive management group, it is really around our risk framework and having cordially conversations around risk and particularly around information management and information privacy. But also in terms of our audit and risk committee, we have a fraud and corruption sub-committee and that's chaired by my Deputy Director-General of Corporate Services and they have a

responsibility as well for a level of assurance and governance in relation to our fraud and corruption framework which would include matters in relation to misuse of personal information as well.

CA That fraud and corruption control sub-committee reports to the audit and UI assessments.

W That's correct, yes.

CA And they measure trends across the Department?

W That's right. So reports and data and some of the data that's available to the Commission in terms of the number of breaches, whether those breaches have been substantiated. Those particular matters are discussed in that committee.

CA So you're looking at particular user profiles when you're looking at that to determine interventions, education and controls that if there should be any adjustments?

W So we would look at – well, what that particular user had access to, that would be what the user profile would actually explain; that's correct. The only other thing I'd say from governance, I don't want to pre-empt anywhere you might be leading, but I guess as the Director-General then my responsibility of providing messages to all of our employees-

CA Yes.

W -I have a regular fortnightly email that goes out to all staff.

CA Have you got an example or?

W I don't actually have one of those. But I do have an example I guess of what I did during privacy awareness week was actually provide an email out to the entire Department talking about that and talking about staff's obligation in relation to use of data and appropriate use of data. And I can table that if the Commission is interested around that.

CA So that general awareness campaign for privacy, that's an annual event?

W That's correct. And you'll see that it talks about in here, the code of conduct and standard 4.4 which talks about information, it talks about the Information Privacy Act. It talks about protecting information. It talks about the use of personal information can be a disciplinary, criminal or a criminal offence as well. Based on the earlier conversation we had I guess one of my learnings for next year is be more explicit around perhaps the Criminal Code and what those actual sanctions might be in relation to that as well.

CA Okay. Thank you.

W Underneath that then is cascaded a range of other emails so, for example, my Deputy Director-General of Corporate Services would send out an email when we have the annual Right to Information Day. And again that happened this year. And again we were quite explicit. An important reminder is to ensure that employees do not access information on Departmental systems that are not required to access, to explicitly meet their work responsibilities. And it goes on about the fact that you are leaving a digital fingerprint every time you actually access that information. Below that then our Assistant Director-Generals would send information and, again, particularly the Assistants Director-General in charge of Human Resources sends information out to his staff that would obviously have access to quite personal information about employees about the appropriate use of that information and how they should or should not be accessing information in relation to that matter as well.

CA Thank you. I tender that document and if it could be read into the record, Chair.

PO Exhibit 32, thank you.

ADMITTED AND MARKED EXHIBIT 32.

CA Now, Mr MILLER is here to speak in relation to specific case studies.

W That is correct. That's my understanding.

CA And discipline in more detail.

W And our procedures around that particular issue, that's right.

CA If I could just touch more globally on a couple of matters and if you aren't able to speak to that, then let me know.

W Sure.

CA Because we've got Mr MILLER waiting. So you're aware of, no doubt, the section 15 of the Crime and Corruption Act?

W Mmm-hmm.

CA If Mr COOK could be shown-

PO Exhibit 8 I think.

CA Exhibit 8.

W Thank you.

CA That requires under section 38 the Department to notify the Commission if there's – UI in particular with what we're talking about now, misuse of information that would be a criminal offence or disciplinary action which could potentially lead to termination. And then the Commission has collated some data across all of the seven subject agencies. And I'll just show you that, those tables, over the space of four pages.

W Thank you.

CA If I could just go back to the teachers union submission and tender that document?

PO Make that Exhibit 33.

ADMITTED AND MARKED EXHIBIT 33.

CA And tender the Crime and Corruption data, the four tables that have just been handed to Mr COOK.

PO Exhibit 34.

ADMITTED AND MARKED EXHIBIT 34.

CA So the first page are the number of allegations which are all there on the second page which is the number of complaints.

W Mmm-hmm.

CA So we'll go to the second page. You'll see that there has been a sharp increase in complaints over the course of the last four years, from 2015-2016 there were eight; and in 2018-2019 there were 37. So that's quite a substantial increase. And then if we go to the third page, the allegations are divvied up and you'll see for the 2018-2019 financial year it was predominantly access only. And then followed by disclosure. So out of the 47 in total, there were 37 – oh, 27 accesses, sorry, and 11 access and disclosure.

And then on the last page, there's proportional breach. And the calculation of that has been from the reports by your agency to the Commission for the complaints, and then the staff numbers from your annual report for the 2018-2019 financial year. So you'll see there that you definitely stand out there as having a very low number of proportional breach, 1,193; compared with the police, 75; and Corrective Services 76; and then the others are all between 265 and 751. Do you think that the extremely low number may be that there is under-reporting occurring due to potentially confusion over what is misuse of information, given the confusion that we talked about with the Education Act providing disclosure with concerns of the person, and then the Criminal Code of being in a sense access only?

W That's a difficult question to answer in the sense of I would have to make assumptions I guess as to why this is not happening. There's been no explicit information provided to me by staff themselves, by any of my senior staff or even by the union, to me directly about why there's a view that those numbers are as they are represented in these tables. I guess the point I would make, however, is that in terms of the information that we provide to our staff there's always areas for us to improve in. We've highlighted the issue here today about the fact that in terms of education staff there's a range of legislation that covers the use of information and the misuse of information. And having – providing more clarity around that I think would be something that would be useful. The question you've asked me is about under-reporting. I mean obviously because of the size of our organisation is much, much bigger than anyone else of the – any of the other organisations that you're looking at, I'm not surprised I guess by the proportional breach. Am I surprised by the number of complaints being 37 on page 4 of the document that you've given me? Um, it comes down also to the context in which most of my staff operate. And so most of my staff, for example, are operating in a situation where they're not in front of a computer, they're actually operating in a classroom teaching scenario. And so despite the fact that we have many entries into the OneSchool the majority of their teaching time is actually spent in front of the classroom, not in front of the computer, unlike me where I spend a lot of my time in front of the computer. Having said that, I think the learning out of this is for us to continue to promote and to be quite explicit about the importance of information security and privacy. But also as you've mentioned the implications and the criminal implications of what actually happens if you don't follow those procedures. I am pleased – I'll just wrap up – I am pleased to see in one sense that there has been increase because I would like to think that's because of the actual training and the awareness that we are providing to our staff in relation to the issues that should be raised.

PO And then that in turn, Mr COOK, might indicate that there hasn't been under-reporting but it is difficult to say.

W That is correct. I can't as the Director-General say whether this is under-reporting because I don't have any information made available to me that people have a sense that there is under-reporting happening. But – and like I said there's has been no key stakeholder that's really raised to me directly short of – I do acknowledge the QTU's submission, but to me personally the issue of this has not been raised. The issue of workload in relation to OneSchool has and we are looking into that into the future about the workload that OneSchool and the entries into OneSchool brings on to staff. But the information security aspect of it has not been raised to me personally as Director-General.

CA Now, in relation to a threshold to discipline, is that within Mr MILLER's purview or do you have a broad sense of what goes on?

W I will rely on Mr MILLER for that absolutely.

CA Just one particular area of that is that where there have been referrals to the police, are you aware of any problems with the police looking into those matters?

W So I'm not aware of any problems. I am aware that, and I don't know the number, but it has been mentioned to me, that in – there are cases where a referral may be made to the police and the police will make a decision that the matter goes no further, that there's no requirement for them to investigate further, which happens across all police forces. I know that happened in Australian Federal Police when I worked in the Commonwealth as well. I'm not – I'm not au fait with the particulars of that or the number of times that has happened.

CA Thank you. You talked about you doing constant messaging and for a preventive function and also those below you.

W Correct.

CA How do you manage the effectiveness of those messages of your senior managers?

W I guess the management is my expectation, again, in terms of the culture. I don't go back and say "Do we have any evidence that your emails have been opened?" I don't ask those particular questions in relation to that. It comes back to, I guess, to the culture. It comes back to looking at the data that you've provided me and whether in fact there's been a shift in any data as a result of the emails or the information that's been provided. But it will also be, I guess, the questions that we have in relation to our policy renewal about how can we actually make these policies better based on any feedback that might have been provided. I rarely get feedback. I rarely get feedback to any of my emails. Sometimes staff will be reply to me, but not many of the 88,000 staff sends me a direct response to any email that I send out. But they know they're regular, they know every two weeks there will be a communication from me directly to them about the matters that are impacting on the Department.

CA And just a couple more things: in relation to the sharing of data, are you aware of the extent that it is necessary for you to share data with other agencies?

W So there is a range of data information as you know. In terms of child protection there's child protection information. There's information that under law we're mandated to provide to child protection, but also to police and all staff are fully aware of that. And we have extensive training in relation to that and guidelines in relation to that. The other thing that I mentioned earlier in my statement was the youth engagement alliance information sharing charter. Which is a charter that's been signed by a range of agencies, including police and health where in each of our seven regions we have what's called a youth engagement hub. And that youth engagement hub works particularly for or

with students that might be disengaged from school and actually may not be in schooling. And it may require us to share information in relation to that particular student to enable us to get the best outcome for that student in terms of returning to education. And this, the charter, which again is a public document, the charter outlines a range of things in relation to that. It outlines implications in terms of legislation. It gives particular examples around each of the eight government departments that are signatories to this about what implications their legislation has in relation to sharing the data. And it has templates and forms provided to enable, whether it be school or regional staff, to get permissions from people to utilise their data for the purposes of ensuring they can be returned into education. And so that's a particular joint initiative across a number of government departments in Queensland. It is a public document, but I'm happy again to table this if that assists the Commission, but it is a public document. It is 66 pages long – or 55 pages long. It is a quite detailed guideline in relation to it.

CA If you could just state the full title of it?

W Happy to do that. So it's actually called the Youth Engagement Alliance. And the main title is Information Sharing Charter. And it is subtitle is Supporting the Reengagement of Young Queenslanders.

CA Thank you. With the Human Rights Act commencing this year, and there being breaches for actions taken after the 1st of January next year, other than what we've talked about today as a way forward, what do you anticipate as the impact on the Department in your approach to protecting privacy?

W So I think the Human Rights Act – and as you know, there is the right to education included in that Act. I think that assists us I guess to again focus on the work that we're doing. That we are undertaking training at the moment across particular our major decision-makers. But the Act helps us I guess look at the material that we have developed to date particularly in relation to some of these areas about information privacy and the management of information and assists us ask the question about in terms of the interaction between the Human Rights Act and what we're currently doing, how well are we meeting the objectives in the Act in relation to privacy and information.

CA And with the Information Privacy Act you mentioned that a few times, you will be well aware of Information Privacy Principle 4.

W Mmm-hmm.

CA Of the storage and security of personal information. And would you be aware that there's currently a matter going through the court process in relation to another agency for that matter, for that issue?

W I'm not sure which one that might be referring to, I'm sorry.

CA The issue we're talking about is vicarious liability.

W Right, okay.

CA So your agency's obligation to ensure that all reasonable steps are taken to protect the confidential information of the public that you store. And that is detailed in the IPP4 at 1(b). And if Mr COOK may be shown a copy of IPP4? I tender that document. 1 (a) (ii) talks about unauthorised access.

W Mmm hmm.

CA As you mentioned in your opening statement that even curiosity breaches aren't tolerated.

W That's correct.

CA And we went through that there could be some confusion of your staff when they're not drawn to the Code and they're only drawn to the Education Act.

W And the Privacy Information Act as well, yes.

CA So other than the steps that we've talked about today to sort of tighten up the deterrent effect that you're already well underway with your educational mandatory training awareness and emails to clarify that for your staff, are there any other – Information Privacy Act talks about all reasonable steps. Are there any other steps that you think your agency could take to further prevent your staff from misusing the information on your database?

W So there's a few things, I guess. I mentioned the audit regime. I won't go into that again. But out of each of those audits comes recommendations for us to consider in terms of our improvement. And as I said there's been a number of recommendations come out of internal audits in relation to things like being more explicit around user access controls and guidelines for the OneSchool software suite. So there's always – and that will be a continual piece of work for us. So, again, we have got a forward agenda for audit over the next 12 months and just based on what I know I think we're looking at user controls again in the next 12 months: sorry, I just can't find the right document. Here we go. So in the next 12 months, for example, in the access management review, user access review, data analytics and business intelligence review, data integrity, school internal alert processes which also would include sometimes confidential information about what's actually happening to a school – a student in a school.

So for us that auditing side of things is quite important because out of that we can then gain learnings about areas that we should improve in. Those recommendations are then monitored through the audit and risk committee to ensure that the management that has agreed, the management section of the Department that's agreed to particular actions, actually ensure that they deliver

against those actions. And so that's the level of assurance for me to ensure that happens. The frontend is the proactive side and we've talked about that for quite a while today so I won't go in that. The backend for me, I'll be blunt, is a challenge in the sense of as I mentioned earlier, to make changes to our OneSchool IT system knowing that there's about 3.6 million hits a day or users a day requires quite a sophisticated outlay in terms of both resources but also in terms of how that will be done to ensure the system actually continues to operate. That is something we're continuing to look at, particularly in terms of changes to technology. So with the changes to technology how can we utilise those changes to technology to actually modernise our OneSchool software. Because as you have mentioned that's our major point of data storage in relation to personal information. We have to balance that with ensuring that the software continues to function in an effective way. But that's one of the things that I know my Chief Information Officer is looking at in terms of what else can we do around OneSchool to ensure the security of the information, but also as you've indicated to provide explicit information to the users of OneSchool about the appropriate use of that information and then the sanctions of that use is actually inappropriate.

CA Lastly, just a very quick question: what processes do you employ in relation to vetting new employees?

W In terms of criminal checks? So certainly criminal checks.

CA Vetting them in general, what do you do?

W So there will be everything from referee checks, their personal referee checks and then it's mandatory for criminal checks. So the Queensland College of Teachers actually does that for teaching staff. From a Department perspective we will do that for non-teaching staff. You were just talking about new employees weren't you there?

CA Yes.

W Okay. So that's the range of vetting that we would do in relation to that.

CA And just one last question back on section 408E, I know we spent a long time on it, but the messaging to your staff you said in your opening statement that curiosity breaches aren't even tolerated. So just moving forward, would it be clarified for them or is it already that for a benefit it could be just mere knowledge that there's something there just accessing only UI be a benefit?

W Sorry, I don't-

CA UI a tangible financial benefit.

W I see. So the misuse of data may be for a benefit of knowing something as opposed to gaining a financial gain? Yes. So in a sense that's the sense of the

curiosity aspect from our perspective as well. So some of the messaging that we do put out to staff does mention that. Could we mention that more explicitly ? I believe, yes, we could.

CA Thank you very much for your time.

W Thank you.

CA I have no further questions, thank you. Mr COOK can be excused.

PO Yes. Thanks, Mr COOK, you're excused. Thanks for coming.

W Thank you.

PO Is it convenient to take the morning break now, Ms FOTHERINGHAM?

CA Yes, thank you.

PO All right. We'll adjourn and come back at midday. Thank you.

HRO All stand. This hearing is adjourned.

END OF SESSION