PO I'll make that Exhibit 19, thank you.

ADMITTED AND MARKED EXHIBIT 19.

CA So on the first page, Mr SCALES, there are the results for the seven agencies, and your one is highlighted. And that's the number of allegations. On the second page it is the actual overall number of complaints, the allegations may be more than one complaint. If we just turn to that. There has been an increase from the 2015-2016 financial year there being 13 complaints, and then 2018-2019, 22 complaints. So it has almost doubled and, in particular, jumped from 11 in the 2017-2018 year. So it is a matter of an area of interest for the Crime and Corruption Commission to look into why that has occurred.

Now, if we go to page 3, that breaks up the allegation types. And you'll see that out of the 39 listed for this year that it is pretty well even, and it is the main source unauthorised access, being 17, and access and disclosure being 12. So they're the two main issues that your agency is looking at.

W Yep.

CA And then on page 4, there's the overall proportional breach per employee with the seven agencies. And, well, apart from the Department of Education being 1 in 1,993, the Department of Transport and Main Roads is sort of somewhere in the middle being 322. That's just an overall.

W Okay.

CA Now, in relation to your organisation, could you please describe the functions that your agency is responsible for performing?

W As I've said in the opening comments, we are charged with getting to a single integrated transport network that's accessible to everyone. As far as the inquiry is concerned, I guess the bigger single part of that will be our TRAILS system, which is the Transport Registration and Integrated Licensing System. We have some 5.6 million licenses on the system, and about 3.7 – sorry, 5.5 million current registrations on the system and 3.7 million licenses. So that's the repository of all the licenses in the state itself. So we do reminders for registration and licensing. We help our colleagues in the police in terms of the road policing command if they stop a vehicle so they can access the TRAILS system and we have an MOU in place for that. And we provide information to the other departments as well on an MOU basis. So if you take that bit which is the focus of this inquiry, I think that's probably the focus, our TRAILS system. The other things that we do provide is you know building the network and planning the network. So the planning side is in the PPI branch and the building side is the Infrastructure Maintenance and Delivery branch with the $23 million capital program over the next four years. So we actually plan the network, we operate the network and we deliver the network.

CA The main focus for the hearings is the main customer database, which is TRAILS, Transport Registration and Integrated Licensing System. And the complementary database for the transport integrated customer application.

W Yes.

CA Could you please describe in general terms the type of private and personal information that your agency collects in relation to members of the public?

W So we have identification information, so that's names, dates of birth and address details. Contact information, which are telephone numbers and email addresses. Travel data for public transport trips, that's on all modes of transport, bus, train, ferry and tram travel. We have images on the system as well for proof of identity and also for driving licences, so proof of age cards. We have some limited personal data for the school transport assistance scheme. And information relating to the legal and traffic matters, such as traffic offences or court protection orders. So that's the information we collect on the TRAILS system.

CA And how would you describe the structure of your organisation in terms of responsibilities for these three areas: privacy, information technology security and information management, and the third one being ethical standards and disciplinary investigations and sanctions.

W Okay. Our governance branch is responsible for leading Information Privacy Policy and that's located within our corporate network. So it provides my agency with advice across the Department and also it maintains the Department's Information Privacy breach register. So that's the governance branch. We have got the Ethical Standards Unit, which is located in the – in that branch but it is an independent unit, it is well-resourced. There are seven members that report directly to me. That is the part of the organisation that will meet section 38 of the Act that you showed me earlier. And our information technology branch leads the information security management system for the Department. My Chief Information Officer is also being called as a witness which will tell you a bit more about that system in due course.

So TRAILS is the system that actually holds all of that information and TICA is the system that actually allows users after they have completed certain mandatory training courses to actually access that system. So in total we've got the customer service branch which is headed up by Geoff McGOFFIN, who is the General Manager also being called to give evidence to this inquiry. We have the transport systems area, which actually does system level policy compliance security. The ITB branch, with Sandra SLATER the CIO heads up. We have got governmental department policy ethical standards and risk management because we have got a pretty mature risk policy at the moment. And we have got internal audit. Now internal audit have got a pretty free range as well and they report up to my audit and risk committee. Now the

audit and risk committee is chaired independently and I'm about to change the independent chair on that. And also has two independent members so that acts as a check and balance. Our colleagues in the QAO also attend that meeting and anything that's reported up through the internal audit system goes to both the risk audit risk committee, but also goes to QAO.

CA Thank you. Do you see any – what do you see as the greatest risks and challenges for managing privacy of information in your agency?

W I mean probably the biggest single risk is our geographical spread and the fact that we have over 100 locations across the State and we're highly transactional. Over the last four years just in the TRAILS system there's been over 63 million individual transactions. So we're very front-loaded on the transactional side of things. And our customers obviously when they provide the data expect us, quite reasonably, to hold that data in trust without compromising our ability to prevent or detect information misuse. And really the big risk is just to make sure that the ethical standards that we set within the Department are met and the Ethical Standards Unit does a great job there in making sure that our employees, the 9,100 of us that are in the organisation, operate to the highest ethical standards.

And one of the ways we do that is "Which Way Would You Go?" which is the ethical standards training which is mandatory and happens every 12 months. So we try and keep, you know, an ethical leadership standard going through the organisation, so every time we have staff turnover they're inducted and "Which Way Would You Go?" is part of that. And I think I've also been helped by the Vincent Fairfax course in ethical leadership because that's given me an extra impetus as well.

CA Thank you. And do you or someone else in your agency regularly review the risks and mechanisms in place to deal with systems, processes and people?

W We have a – that's me and the executive leadership team. We have an active risk register. And the risk register is validated every year. And this year we did it using KPMG. So I use an external agency to help validate the risk. And once any risk is detected we look at what the mitigation measures are and also how that might be eliminated in the future. But the audit and risk committee, as I said earlier, Counsel, that's chaired by an independent person, there's two independent members on it, I'm refreshing the chair this year. And I also refreshed the members that are on it from my side of the organisation as well.

So we've got strategic risks. We make sure that they're identified, assessed and managed and mitigated. And it's a living breathing document. So we look at it every year and make sure that every time we get a risk we make sure it is assessed and built into the system.

My Chief Operations Officer can give greater insight in terms of the Department's information security management system. And for the future I

think one of the bigger challenges is going to be cybersecurity because we're helped by the fact that the TRAILS system is on its own main frame, it is a secure system, and access to it is pretty tightly controlled, but cyberattack on our Department is pretty prevalent. We get lots of phishing emails, for example, and where we use the QGCIO, the Queensland Government CIO to help us in any attacks on that side of things. So I think going forward cyberattacks are going to increase so we need to be increasingly vigilant. As far as the organisation is concerned we need to maintain our ethical leadership and also maintain the training programs that we put in place.

CA Thank you. And to what extent do you consider that privacy breaches by your staff impact upon your agency's ability for it to perform its functions?

W I think any privacy breaches are very much a concern to me and I take each one of them seriously. I think they have the potential to affect the organisation's reputation. So anything that we can do to minimise that is obviously paramount and right at the top of my agenda. But if Queenslanders don't give us the information, then we can't provide the licensing and registration function. So we have got a substantial focus on building and maintaining an ethical culture. So the ethical culture in the Department is really important to me.

CA And you've mentioned reputational harm as a potential consequence. Would there also be a flow-on effect, say, customers not wanting to use your online services or your applications?

W We're not seeing that. In fact the online services are increasing year on year. And the more services we put online the more people seem to want to use them. But there are – in the 90 customer service centres that we've got, there are a lot of people that want a face-to-face interaction, but we're seeing a lot of people now moving into the online service. I'm not seeing any diminution of people wanting to do that. In fact it is increasing.

CA And have you conducted any customer surveys specifically in relation to privacy?

W Not necessarily in relation to privacy, but we do customer surveys all the time. We monitor the customer service in our customer service centres on a regular basis and regularly get good scores. We have a customer services branch that looks after that and Mr MAGOFFIN will be able to give you much more detail. But two weeks ago we won a national award for customer service.

So it is something I'm really very passionate about. And my definition of customer service is meeting customer requirements first time, every time. Which means that you've got to talk to your customers in order to do that. So we do lots of surveys but not seeing anything about privacy that's being raised in that area at all.

CA Would it be an area of focus for you going forward for a survey in relation to privacy, particularly given the Human Rights Act being enforced as of the 1st of January next year?

W I don't think so. On the privacy side you've got a couple of pieces of legislation, one State and one Federal that actually, in my view, adequately and sufficiently address the privacy issue. But on the human rights side of things we are looking at our Acts within the Department, how the Human Rights Act will actually impact on those. On the privacy side, I think we've got those two pieces of legislation which are pretty powerful so I don't think the Human Rights Act will directly impinge on that.

CA In relation to organisational culture, you've touched on it, and how do you reinforce that culture within your agency?

W Yes, I'm a highly visible leader. This year so far I've done 90,000 kilometres, I've seen 1,600 in face-to-face interactions with my staff. I do things called D-G roadshows where I get out and meet the staff and also give them an update on what we're doing. So I do D-G roadshows. We have D-G messages. One's gone out today in terms of the bush fires that are outside but also Remembrance Day, for example. We've got active Yammer groups. So Yammer is like a sort of social media internally focused of the 7,000 permanent staff we've got full-time equivalent staff we've got, sorry. There's over 6,000 of us on Yammer group. So we got Yammer groups in operation as well.

We do ongoing mandatory training and ethics with "Which Way Would You Go?" but also the Ethical Standards Unit goes out and does its own training as well. They've done 21 training courses this year across the State. And seen probably just less than a thousand people. We do proactive auditing. We do, I think, strict enforcement of it all.

So any serious allegations are investigated by the Ethical Standards Unit and then we take action from that. But we have done really five major things in this area, training and education, we've been very strong on that. Process changes where required; policy changes where required; we've got lots of assurance and systems changes where required.

So a lot of it is the D-G and the executive leadership team being very visible. The executive leadership team will also do their own messages. And below that the senior leadership team, there's 41 people in that, they will do their own messaging as well. So cascading down from me, you've got executive leadership team, senior leadership team and then there's a greater leadership team which has got about 800 people in. That's at AO8 level and above. And two weeks ago I did a presentation to them on a whole range of things. So I'm a very visible leader and I think you've got to lead from the front. So, to summarise, it's visible leadership, it is reinforcing that leadership and it's also getting the face-to-face contact. But not just me, the executive leadership

team do it. But on the ethics side Trevor Chippindall in that unit goes out and does targeted courses there and he did 21 this year so far and seen about 1,000 staff. So all of those things together keep it going. But you can never stop learning and that's why I did the Vincent Fairfax fellowship ethical leadership course because that is the primary one I think in Australia and it was set up 25 years ago by the Fairfax foundation who – or Mr Fairfax had got pretty fed up with ethical failure he'd seen in business. So he set this up. And I was in cohort 24. And cohort 25 is going through now. And the people on that are, you know, senior policemen, defence, private sector, public sector, not for profits. So it is a really good cross section of people that go through that.

CA And would you say that your staff have a good understanding of the purpose for which they can access your databases?

W Yeah, definitely. And we re-inforce that with the mandatory training "Which Way Would You Go?", and then there is all the TICA training before they get there, and then there is refresher courses. So all of the courses put together and the fact that they're refreshed and monitored, I think, does help reinforce that.

CA You spoke about the – from the top-down approach. With your executive and senior managers, what are your expectations in relation to them communicating messaging to their staff to prevent misuse of information?

W I think we expect them, I expect them to be as visible as I am, but also to make sure that they're operating in an ethical manner and take appropriate action when it is necessary. So we're a very transparent organisation, so our communication systems are quite – I'd like to think that we're sophisticated, but that sounds probably wrong, but actually get to all the right places in the organisation. And just as an example what we do is when we get a new intake of people, I write individual – well, I sign individual letters to them, and then we have an induction course, where myself and the senior leadership team, or the executive leadership team are all present so we can actually tell the people when they come into the organisation what we expect of them, and we keep on reinforcing that.

So with section 38, that's the Ethical Standards Unit's major role. So they act for me in making sure that the Commissioner and his staff are appraised of anything that we detect.

CA For the reporting of allegations, to what extent do you think that misuse of information is reported within your agency?

W Well, the interesting fact is when you showed the uptake on this, I think why you show the misuse of confidence information trend and all this is going up on complaints, I think one of the reasons on that might be the Ethical Standards Units going out and actually you know alerting my staff that it is okay to make a complaint. So I think, basically, because we're a transparent

organisation, people have reported to the Ethical Standards Unit will then report that to the CCC, and the CCC will either investigate themselves or bounce it back to us.

CA And to what extent – you mentioned it earlier in passing – to what extent is it necessary for your agency to share data?

W Oh, okay. We have a number of MOUs with various agencies. Obviously the police and the Road Policing Command, with SPER, State Penalties Enforcement Registry, because we collect data on people that don't pay their tolls. National heavy vehicle regulator, we share information with them. Department of Education, we share information with them on the School Transport Assistance Scheme. So we share the data that we've got with a number of agencies, and each agency and ourselves we have an MOU in place.

CA And are you aware of your agency placing any particular security or privacy protections around vulnerable members of the public; for example, victims of domestic violence who are concealing their location or details from a former partner?

W Well I'm a champion against domestic violence. I just don't think it is right that two women a week are killed by perpetrators in Australia. So we have a system in place which is called a Customer Records Suppression Service. So if a victim of domestic violence has a court order, we can suppress the information at code level 1 and we can suppress the information so that only a small unit within the customer service branch can see that data. So the police can't see it, and no external agency can see it. And if anybody tries to look at it, it sets a flag off, and then we'll investigate that. So that's level 1. That also includes we can suppress key staff within this agency where the Commission is, so CCC staff. We can suppress information on serving police officers or anybody else that meets that criteria. So that's level 1, that's entirely suppressed.

Level 2 is we can suppress somebody's information if they're come in with a stat dec, a statutory declaration. So that's level 2. But the issue with that one is that the police and others could see it if they had a looked at it. So level 1, which is usually domestic violence cases, or key staffing, key locations or key agencies, there's only the unit within the department can see that.

CA How large is that unit?

W I'd be guessing, maybe three or four people, because there's only 683 records in there. So there's not that many. On domestic violence, on level 1, there's about 158 people located in that. So it is only a small unit. But what will happen is that we don't necessarily advertise that service, but our partner agencies that are looking at domestic violence know about it and do point people in that direction.

So at level 1 we can suppress and you can only see if you are in the department. Level 2, our colleagues in the police service could still see it.

CA And with level 1 you said that there is a flag every time the record is accessed?

W Yes. If somebody tries to access it they won't get anything out of it, but will set a flag off.

CA What about the people within the small business unit when they access those records?

W That would set a flag off as well. It is self-policing. And the other thing is that if we got a court order to release that information, or if the individual's records that had been suppressed gave us written permission to release, for whatever purpose, then we'd do it. So it merely is targeted at domestic violence victims and other people.

CA And that flag goes to – a report is produced and goes to where?

W You'd have to talk to Geoff MAGOFFIN about that directly. But all I made sure as the D-G and a champion against domestic violence, was that we had that system in place, but-

CA I'll raise that with him later.

W Yeah, I think so. I don't think we actually promote it, but the agencies that we deal with do know about it.

CA Now, a few years ago there was Operation Danish, which I don't intend to go into any detail with you, there's Mr MAGOFFIN later on in the week, but that was a situation where there was a Customer Services Officer who accessed and disclosed information for financial gain. And she was punished for that. Did you want to talk to that at all in a sort of global sense?

W Yes. I got a very comprehensive and very helpful letter on 24th June 2015 which was very detailed and indicated areas where we could tighten our systems up and also change systems to make them much more robust.

CA Where was that letter from?

W It was from the CCC straight to me. So that was 24th June 2015. I responded on the 17th of August 2017, where we'd actually undertaken, from when I got the letter to when I responded back to the CCC, a huge body of work in eight major areas. So we took what the CCC investigation had said, we took the letter of 24th June 2015 and we did a lot of work which I responded to on the 17th August 2017. And then on the 4th October 2017, I got a response back from the Crime and Corruption Commission. I would just like to read out the

last paragraph and read it into the record.

CA Yes.

It says, "The CCC does not require any further reports on these matters from TMR, and the CCC acknowledges the positive steps that have been taken to date by TMR to implement the recommendations."

And that's all about Operation Danish. Now, that was on 4th October to me. So all of those three things are on the record. So Danish happened, we got a very helpful letter with lots of attachments. We implemented everything we could implement. I put it back to the Crime and Corruption Commission on the 17th of August 2017. And we got the letter on 4 October 2017. But Mr MAGOFFIN will have any details you want to pursue, but from a D-G point of view, it was a very helpful letter we got, and we acted on it and we got a good result, I think, in the end.

CA Thank you. In relation to prevention from the issuing of general warnings, you touched on that earlier, do you send emails to all employees as part of that?

W On general things, if you take the Information Privacy Week, which we promote every year, this year it was on, I think, the 12th to 18th May. And we do that in conjunction with the Information Privacy Commissioner. So every year we actually say to the whole of the workforce "It is information privacy week, and this is what we expect." We highlight the information that we've got in trust. So we promote it like that. Now, that's done on – through the Customer Service Branch. And Mr MAGOFFIN will give you a lot more details on that on the things we do, like toolbox talks. We've got posters. There's the – so the D-G message I put out. We just make sure we reinforce that. And that happens every year. So part of that will be on emails. Part of it will be on, sort of, face-to-face, and part of it will be through posters.

CA Yes, I will speak more about that sort of thing with him. I do have an email that your organisation has provided to us, which was from 26th September 2017 from Mr MAGOFFIN. I'll just show you that email.

W Thanks.

CA Is that the type of communication you send out?

W Yes. And I'd forgotten the exact details of this. And I'll just read it out for the record. It says, "When it comes to information privacy, a peek is a breach." So that was part of the campaign at that time, in 2017, but it also goes to our responsibility training, which is refreshed on a regular basis. And we actually measure people's attendance at those courses. Accessing Customer Records Policy, which is also detailed in here, which is mandatory training. But, I think, probably one of the things that I am very proud of is "Which Way

Would you Go?" the ethical training course. And I'm looking up now as part of the work I'm doing with the Vincent Fairfax Fellowship to see how we might improve that and also provide, maybe, communities practice within the organisation. So that is an object example, you know, "A peek is a breach", what the Customer Service Branch will have been doing. But it will have also been toolbox talks, so, you know, getting people around probably with a cup of coffee and just explaining what the circumstances on safety and what we require our people to do.

CA And I notice in here you have – well, Mr MAGOFFIN has let staff know that the possibilities of the range of consequences from misuse of information include disciplinary action and criminal conviction.

W Correct.

CA I tender that document.

PO Exhibit 20, thank you.

ADMITTED AND MARKED EXHIBIT 20

CA Does your agency have a warning on the log-on screen prior to being able to access the database?

W I would be guessing. That's one for Geoff really, Geoff MAGOFFIN. I would think that we'd use lots of things like that, because if – I just take my own system when I log on; it comes up with a standard warning and, you know, you've got to do OK and then go into the system.

CA Yes, that warning, does that – that warning is on every UI-

W Well, it is on mine, so I assume it's on everybody's yes.

CA Does it include the range of consequences being disciplinary and criminal action for misuse of information?

W I would say yes, but I haven't read it for a long time. But I would say yes. But I think that's probably better addressed to Mr MAGOFFIN, or to the CIO who is the architect of that message. That messaging will have that, I think, at the bottom. But to your point on the access to TRAILS through TICA, TICA will have a different screen I would have thought, but, again, the CIO and Mr MAGOFFIN should be able to answer that for you.

CA Thank you. Just moving on to the policies that you have.

W To the what, sorry?

CA A couple of the policies that you have.

W Yes.

CA There's the Information Privacy Plan which has been updated once in the last four years, including this year. And then the Information Security Policy which has been updated three times in the last four years. How often, as a preventive measure, do you think you should be updating your policies and plans?

W Well, part of the overall risk register, which means that at least once a year we look at the risks and see if we need to update the policies, and that's why there's different timetables on what you've said. Also, our internal audit function will look at various areas of the business. I know that access to the TRAILS system was audited in April of this year, and that might, once it has been through the Audit and Risk Committee, that might trigger another review of that particular policy.

I think the whole point of it is the suite of documents that we've got are living, breathing documents. They're not set and forget. And we try and make sure that each document is as accurate, relevant and as timely information as we can possibly make it. So we look at that, at least, once a year, and then we probably take it from there.

So, effectively, what you've got is a whole series of checks and balances. And I say that the Audit and Risk Committee is chaired by an independent external, with two independent members on it. And when we review enterprise risk register, we get external support, which this year was KPMG. And we have in the past used, I think Deloitte to look at other bits of the policy.

So I don't just rely on the internal audit. I don't just rely on the Audit and Risk Committee. And the Audit and Risk Committee report's also seen by the Queensland Audit Office. So I try and use check and balance from externals as well with a fresh pairs of eyes.

CA Thank you. Can Mr SCALES be shown the Access to Customer Records Policy?

W Thank you.

CA I tender that document.

PO Exhibit 21.

ADMITTED AND MARKED EXHIBIT 21

CA I'd just like to go through this policy. It appears to have some very good content that could be used as a model for other agencies. If we go to point 6.

W On Background?

CA Background.

W Yes, got it.

CA Talking about encouraging public trust and staff by displaying a high standard of integrity. And there's a very good explanation – sorry, definition of what misuse of information unauthorised and authorised access is in a document.

W Yes.

CA And then just going to number 10, that's part of 10, the authorised access and the unauthorised access-

W Yes.

CA -it is clearly spelt out and easy to read and has good content. And then it explains at 10(i) to (k) that authorised access is by using a unique password. And then at point 11, you let staff know that there's proactive auditing to monitor their use.

W Yes.

CA Do you, other than in here, reinforce to staff that when they log on, use their password, that their use is being monitored?

W I think that's part of the general training that we do. But, again, I think you will probably get more detailed information from Mr MAGOFFIN and the Chief Information Officer.

But I think it is part of the culture that we're building up so that we know there's a strict policy of compliance. And this helps crystallise it. And you can see on the authorisation page, Counsel, at the front where the whole thing started off in 2013, in May, and then it has been reviewed, and then updated.

So, again, what I'd say with this document and the other documents in the suite, that is the subject of this inquiry, is they're living, breathing documents. And if somebody came up from outside, say, on cyber policy, or a cyber attack that we could mitigate, that would go in there as well. So each time we update it, we try and make it as current as we possibly can.

CA And also there it talks about the monitoring, going to the extent of showing unusual trends of use.

W Yes.

CA Do you have any more information about that—

W Unusual trends could be accessing data sets from the same family, like SMITH. It could be accessing outside of normal working hours. It could be accessing ethnic groups. It could be accessing, say, more than 10 downloads out-of-hours. So those sorts of things would set a flag and then would be investigated. But, again, Mr MAGOFFIN would have more detail. But those little examples I gave you, are the ones I know that do exist. And the one that we come back to – sorry, we can go back to, which is the level 1 and level 2 security for domestic violence victims, that would certainly set a flag.

CA Yes.

W No matter when that happened.

CA And then at Appendix A are the possible consequences of misuse of information. It clearly stipulates there section 408E of the Criminal Code as well as disciplinary action.

W Correct.

CA There is one area that I wanted to raise with you, though, on this document, if you could elaborate. At Appendix A, under 16, it talks – there's a couple of case studies, and one of them is a case study that we already had, or I'd like you just to check that it is. If the witness can be shown the letter? Are you familiar with that case study at all?

W No, I'm not. And the reason is basically because the disciplinary matters, I'd expect my officers to actually undertake all that discipline. It wouldn't get to my level. So I don't think I can help the Inquiry with this particular case, but I'm sure Mr MAGOFFIN would be able to do that.

CA I'll tender that document now, if that's okay.

W So I can't – I can't – I don't have any knowledge, I'm sorry.

PO Exhibit 22, thank you.

ADMITTED AND MARKED EXHIBIT 22

CA In relation to that, given that you don't know the details of it, we can raise it with Mr MAGOFFIN, but if I just talk about the factual circumstances and we can confirm that with him later, so saying in the abstract, the one that you have here, the one where in the document at Appendix A there was termination. I believe it is the first one.

The first case study in the Access to Customer Records Policy. A TMR employee was involved in a road incident with a member of the public. The employee contacted a work colleague who had access to TRAILS and asked

them to access the customer records using the registration number. The registered operator's details, including their phone number, were passed on, who then threatened and intimidated the member of the public. And then the consequence was a formal reprimand and a reduction in pay.

In that instance, the more senior employee who accessed and disclosed the information to the more junior was given a pay point reduction, as it is mentioned in here. And the one who was given the information, involved in the road rage incident and then threatened and abused a member of the public, using that information, was terminated. Doesn't that show that the disciplinary action in relation to the more serious misuse offence of accessing and disclosing to a person who they knew there is a risk of using that information to cause physical and/or psychological harm to a member of the public, isn't that a serious matter where it should not lead to just merely a pay point reduction?

W I think that's – well Mr MAGOFFIN will be the delegate that would have all the background and everything. So it wouldn't be me that actually took that decision. So without all the background, you'd really have to – and I've got no idea what the detail of this is so – but Mr MAGOFFIN will be able to help you with that, I'm sure.

CA But to put this in the policy, isn't it having a – not a good deterrent effect if the staff know their conduct will lead to a not very harsh disciplinary action?

W No, I don't agree with that. That's just one case, really. And as I said before, just in context over the last four years, there's been 63 million transactions on the TRAILS system. I think on that one issue you'd really have to talk to Mr MAGOFFIN. And I think he would be the delegate. And it is up to him what action he might or might not take. But the very fact that we have it as a case study will indicate that we do take it seriously. And I do know that from – from being where I am, that over the last four years we've actually referred 26 issues like this to the police. So that might be one of them as well. I don't know. So we do refer things to the police which are serious, which is not in this detail in the case studies. But the document itself is, as I say, is a living and breathing document, it is there to educate our staff and to make sure that they do the right thing. I think largely they do that.

CA But for that particular case study, on the facts in the actual policy, to show to staff that if there's a General Manager who accesses and discloses information on the system to another employee, involved in road rage incident, who then uses that information to threaten and intimidate a member of the public, and they are only given a formal reprimand, isn't that sending a bad message?

W You'll have to talk to Geoff MAGOFFIN about it, because I'm not the delegate, and he would have dealt with it. Each case is dealt with on its merits. I don't know what's behind it. I haven't got the detail with me, but I don't agree with what you're saying at all.

CA Just moving on to Information Privacy Principles in the Information Privacy Act.

W Yes.

CA And there's Information Privacy Principle 4, IPP4. If Mr SCALES could be shown Exhibit 13?

W Thank you.

CA You'd be familiar with that?

W Yes, I am familiar with that.

CA So there's an obligation by the agency, by your agency, to make sure that the public's information is stored and secured, and misuse of information is particularised at subsection (4)(1)(a), and in (4)(b) the agency needs to take all reasonable steps to prevent unauthorised use or disclosure. You may be aware that there's currently a matter involving another agency going through the courts specifically on this issue. And what steps does your agency take to ensure that all reasonable steps are taken?

W Okay, just on IPP4 then. What we encourage our staff to do is adopt a clean desk policy; so in other words, we make sure every time they, sort of, pack away overnight, everything is off the desk and locked away. We use secure printing, so the printing is watermarked. So anything we print off on that is watermarked as well. We lock our screens in absence from their workplace as well. So if they're going to leave the workplace for any length of time, they actually lock the screen and log out. We also consider security measures when we do privacy impact assessments and all new programs and projects.

CA Could you just expand on that, please?

W Which one?

CA The impact assessments on new projects.

W So if you take a good example, there is the CORAL project, which is our new digital licence. We're doing a lot of work now with the Information And Privacy Commissioners to make sure that before we actually take the first step, we've actually got them on board so that they can make sure that we're heading in the right direction, with the right security protocols, the right access controls, and we're not bringing them in at the end when we've actually got the projects set up. So CORAL is a really good example of that. That's our new digital licence. So we have actually within our ICT branch, which our CIO can tell you about in more detail, we have got an Information Security Unit who will conduct penetration and testing and also security risk assessments.

So on IPP4 we do a number of things. One is all the housekeeping stuff, which is, you know, lock the screen, make sure you have a clean desk policy, make sure that all the printing is secure. And for the future, we actually assess it to, you know, to a risk level using the Security Unit inside the ICB branch. But, secondly, we actually bring the agencies in right at the start of any new project just to make sure that they're not being added on at the end. So they can add value on all the way through. That also includes discussions with key agencies inside the public service - pardon me - like Treasury, DPC, the police. Probably that would be it. Maybe the planning side. Sort of make sure that we're all moving ahead in the right direction and taking as much advice as we possibly can. So on IPP4, I think, we can actually demonstrate that we've taken some really positive steps on that one.

CA And also one part of that is to assess the possible adverse consequences on an individual case-by-case basis, and you have that flagging for highly sensitive cases.

W Yeah. I think, the only thing I'd say on that one, I think I've said it before, is that it's not something we advertise, but with the – on the highly sensitive side of things, the agencies that we work with, particularly on the domestic violence side, know it exists. I suppose other people will know now since this is being televised, so-

CA Thank you, Chair. Thank you.

PO Thank you. Mr HUMBLE, do you have any questions?

LR Just one question: Mr SCALES, you mentioned the Ethical Standards Unit and its ultimate responsibilities. Is it the case that that Ethical Standards Unit has itself been the subject of audit?

W Very good question. It has been audited by the CCC three times recently. And it has got the highest result from that, which is satisfactory in all three cases. So it is independently audited by the CCC. Thank you for that. I had forgotten that.

LR Thank you.

PO Thank you. Anything arising out of that?

CA May Mr SCALES be excused?

PO Yes. Thanks, Mr SCALES, for coming. You're excused.

W Thank you, Commissioner.

END OF SESSION