

## STATEMENT

I, IAN JOHN LEAVERS of C/- 217 North Quay, Brisbane in the State of Queensland, state as follows:

1. I am the General President of the Queensland Police Union of Employees (QPUE).

### Introduction

2. The QPUE is a registered industrial trade union whose membership essentially comprises non-commissioned Queensland police officers, i.e. of the rank Senior Sergeant and below. Watch house officers (civilians), Police Liaison Officers, Community Police (TIPSO) officers sworn under special legislation for their respective communities) and QPS band members are also eligible to join the QPUE.
3. As at 31 October 2019 the Union's membership stood at 11,776, being approximately 98% of the non-commissioned QPS officers currently serving today.
4. The objects of the Union are to protect and advance the employment, industrial and legal rights of its members.
5. I have been involved with the QPUE since 1997. Prior to serving as General President, and whilst serving as a fulltime police officer, I also served as a branch official for the Ipswich police district from 1997 through until 2005 and then the Southern region representative until 2009 when I commenced as the General President on the 1<sup>st</sup> July 2009.
6. I am a Sergeant of Police having been sworn into the Queensland Police Service on the 27 October 1989 and have served in various positions, including 1<sup>st</sup> response (General Duties), Criminal Investigation Branch, the Juvenile Aid Bureau (Child Protection), Traffic Branch, Forensic Crash Unit as well as being involved in training areas involving Operational Skills Training (OST).
7. My experience both as a police officer and union official over the last 30 years has given me significant exposure to issues surrounding the use of confidential information within the Police Service, and in more recent times, the steps taken (by the Crime and Corruption Commission and the Queensland Police Service in particular) to enforce the proper use of that information.

---



IAN JOHN LEAVERS

8. I recognise that the QPS is uniquely positioned amongst all government services in the breadth and sensitivity of the information it holds within its electronic databases. Information held by the QPS goes not only to issues of national security and public safety generally, but also involves very sensitive information of a personal nature, such as details of an individual's criminal history, complaints made by them and about them, and other sensitive topics such as domestic violence and mental health issues.
9. Recognising that, the QPUE is supportive of appropriate steps being taken to ensure that such information held by the QPS is handled with all necessary confidentiality and discretion, and that any misuse of such information is dealt with consistently and appropriately.
10. Having said that, for the reasons outlined below, I do hold concerns in relation to some aspects of the current regulatory environment concerning alleged misuse of electronic information held by the QPS. In particular, my concerns can be summarised as falling under the headings of:
  - (a) Shortcomings in policy guidance and training for police officers, and
  - (b) The relatively recent practice of charging police officers criminally for alleged misuse of the police database, which in some instances has represented (in my view) an overly prescriptive and punitive response to the behaviour in question.
11. These matters will be discussed further below, together with some suggested initiatives to assist in the appropriate and proper management of the access and release of confidential information by police officers, and the steps that should be taken to address any misbehaviour in that regard.

**Policy issues**

12. The current QPS policy framework in respect of confidential information is far from perfect – in fact it can be described as cumbersome and ambiguous in parts.
13. The current level of policy instruction for police in relation to the appropriate (and inappropriate) use of computer information is too broadly targeted. In my view a far more direct, unambiguous and instructive policy position needs to be taken by the QPS.
14. This is not a new issue – in 2000 the then Criminal Justice Commission held public hearings and published a report, *Protecting Confidential Information*, which noted (at page 57):

*During the Inquiry it became clear that there are differences of opinion as to just what is an appropriate reason to access the computer system. The QPS should*

---

  
IAN JOHN LEAVERS

## CCC EXHIBIT

make a public statement on whether it is appropriate for a member to look up records:

- Of a person with whom they are wishing to associate or are considering a relationship
- Of a friend or relative where involvement with the police is suspected
- Of an individual who has been mentioned to them and about whom they are curious
- Of an individual who is about to be employed by a friend or relative
- To check vehicle-registration particulars before buying a vehicle to determine if it has been in an accident or in fact stolen
- Of prospective neighbours to see if they are part of the 'criminal element'
- As part of a self-training exercise

Any decision by the QPS on what type of access is accept must be clearly communicated to members.

15. To my knowledge, the QPS have not provided this type of clear policy guidance that the CJC called for almost 20 years ago. Rather, the published policy documents rely on more generalised notions of conducting searches for "police-related business" and the like.
16. Existing policy direction is contained across multiple documents, making review and consideration of such policy much more difficult. Those publications also use differing language and adopt differing tests too, again making compliance (and enforcement) more problematic.
17. Currently, within the QPS, relevant provisions can be found in at least these places:
  - QPrime log-in screen;
  - Information Management Manual;
  - Standard of Practice, Professional Conduct;
  - 2013/05 Procedural Guidelines for Professional Conduct, and
  - Management Support Manual.

### QPRIME Log-in warning

18. When logging onto the QPS police system, a screen is shown, titled 'WARNING – CONDITIONS OF ACCESS TO AND USE OF THIS COMPUTER SYSTEM'.
19. The contents of that warning are:

---



IAN JOHN LEAVERS

## CCC EXHIBIT

1. *Access to and use of any information on this computer system is for authorised users only. Unauthorised access and use, e.g. the use of another's USER-ID and Password is strictly prohibited. By accessing or using this system you are representing that you are an authorised user. You are NOT authorised to access information for personal reasons.*
  2. *The information contained on this computer system is confidential and must not be disclosed to unauthorised persons. Improper disclosure of information is an offence against section 10.1 of the Police Service Administration Act 1990.*
  3. *Making unauthorised copies of software is a criminal act and can expose you to punishment or civil claims. Use only authorised software.*
  4. *Details of all transactions, including User-IDs are automatically recorded by the computer and can be retrieved. By accessing and using this computer system you are consenting to security monitoring.*
  5. *Malicious entry of false information is strictly prohibited. Any member who maliciously enters false information may be liable to be dealt with for misconduct.*
20. It is noteworthy from this warning that:
- a) The language is of "authorised" and "unauthorised" use, although no practical guidance is included as to what constitutes such authorisation;
  - b) The reference to criminal consequences only refers to the provisions of the PSAA, not the Criminal Code.

### Information Management Manual

21. Section 4.11.4 of the Information Management Manual covers the policy on Authorised Use of ICT Facilities and Devices. It states

*Unless otherwise authorised in this policy, QPS ICT facilities and devices must only be used for official QPS business and professional research and development.*

*Official QPS business includes:*

- *Using ICT facilities and devices for work-related use*

---



IAN JOHN LEAVERS

## CCC EXHIBIT

- *Using the internet to access work-related information*
- *Sending emails to colleagues as part of official duties*
- *Sending emails outside of the work environment as part of official duties.*

22. I note here that the language of this policy is couched in terms of "official police business", which is further defined by reference to "official duties" and "work-related use". Again, no practical examples or guidance is included. In my view that type of policy prescription provides little guidance or assistance for operational police. It is a far cry from the sort of clear policy provisions recommended by the CJC in 2000.

### Standard of Practice

23. Section 16 of the Standard of Practice deals with the Improper Use of QPS Information:

*When dealing with official or confidential information of the Queensland Police Service, members are not to access, use or release information without an official purpose related to the performance of their duties.*

24. Here is a new test again – "official purpose related to the performance of their duties". Once again, no practical guidance is given as to what this term means.

### Procedural Guidelines for Professional Conduct

25. Section 3.10 of the Procedural Guidelines for Professional Conduct expresses it differently again, stating:

*The unauthorised and improper access, use or release of investigative information to a suspect or accused person is not permitted.*

26. 'Improper' is defined as 'anything that is not in accordance with propriety of behaviour or conduct suitable for a particular purpose, person or occasion'.

### Management Support Manual

27. Chapter 5.6 of the Management Support Manual governs the disclosure of QPS records and misuse of information from QPS computers. Across about 60 pages of policy, the Management Support Manual sets out the limits of disclosure and the Information Privacy Principles as applicable to the QPS.

28. Section 5.6 deals specifically with the 'Release of Information'. In the main, the policy is unhelpful in assisting police deal with many practical issues of disclosure, simply referring officers to other policies (those mentioned above). Little by way of specific guidance or examples is given. For example, at section 5.6.17 headed "Requests by members for

---



IAN JOHN LEAVERS

information about themselves", the policy simply states that "... information contained in such documents as personal files should be provided to members with restriction only in very limited cases." Officers are then directed to refer to the Access and Disclosure of Human Resource Information within Personnel Administration of the Human Resource Policies.

Commissioner's Circulars

29. In March 2016, December 2018 and November 2019 the Commissioner of the QPS emailed all members a 'Commissioner's Circular' on unauthorised QPRIME access.

30. In March 2016, the email stated "*If you use QPS computer systems to access information and it is not for a purpose connected with your duty, the conduct will be considered misconduct. Consideration will also be given to criminal charges being applied.*

In the December 2018 circular, this was adjusted to: 'Only using police information for an official purpose, in connection with our official duty'

31. In November 2019, Commissioner Carroll stated:

*Accessing QPS confidential information without a purpose related to your official duties is both a criminal offence and misconduct. Every information misuse complaint will be considered for criminal charges in line with the DPP Guidelines, assisted by the information misuse guidelines. Curiosity or personal interest is not an acceptable reason to access QPS information.*

Reflections on Current Policy

32. In my view there needs to be a rationalisation of the amount of policy prescription provided to police in respect of this issue, and it needs to be presented in a clearer, more consistent, and more instructive format. The QPUE has raised this issue previously with the QPS – I understand the QPS's position to be that the circumstances and scenarios in policing are too diverse to have a more definitive policy. My experience in recent years though, as the CCC/QPS enforcement of these issues has gathered momentum, is that well-meaning members are commonly confused as to the scope and extent of the application of the policy.

33. The following examples, which have come to my attention as part of my Union duties, serve to illustrate:

---



IAN JOHN LEAVERS

*"Example 1: An officer was doing a bail objection in respect of an offender he had arrested. He was aware that offender had previous convictions and had previously been the subject of bail objections by other police. He proposed searching for those previous bail objections to assist him in the compilation of his current objection but was advised by his supervisor that that previous matter was unrelated to this one, and he should not access it, or otherwise he might be guilty of computer hacking.*

*Example 2: It has traditionally been a practise that junior police, when learning how to prepare paperwork (such as police court briefs), are referred to the previous work of an experienced colleague to learn 'how it's done'. It is now thought that an officer accessing the details of a matter in which they had no involvement, purely for training purposes, might fall foul of the current rules, and therefore that valuable source of learning and instruction has been curtailed.*

34. In providing these examples I am not seeking to debate whether the fears expressed were correct or incorrect. Rather, I use these as illustrations of the confusion and concern felt by serving police officers in relation to the scope and extent of the policies and laws governing the misuse of electronic information.

#### **Training issues**

35. Closely allied with concerns about the adequacy of policy is the lack of meaningful training for the police in this area.
36. What is needed is a more concerted campaign of education and training, allied with clearer policy, to ensure that there are no "grey areas" in respect of what a police officer can and can't do in using the police computer.
37. To my knowledge the only compulsory training provided to Queensland police officers is provided during their time at the Academy and when they first obtain authorisation to use QPrime. There are on-line learning modules available for operational police, but they are not compulsory.
38. The lack of effective training across the QPS was highlighted in recent evidence given by Superintendent David Johnson, who served as QPrime Business Manager from 2011 – 2017 to the Brisbane District Court. In his evidence Supt Johnson said:
- The two main sources of QPS rules for QPrime access were the Information Management Manual (IMM), and the Standard of Practice (SoP);
  - The IMM is not something mainstream police would be expected to be across;

---



IAN JOHN LEAVERS

## CCC EXHIBIT

- In fact, he wouldn't know many frontline officers who would be aware of the IMM;
- The SoP is something that at times is sent out to police by way of a group email;
- There's no auditable trail or requirement for use or testing on the SoP.


A copy of that evidence is **attached** to this statement.

39. In my view, the QPS needs to roll out a more considered and intensive training programme to ensure that all officers are adequately schooled in this area. Group emails and pop-up warnings on computer screens are of limited value, I think. More comprehensive training is needed.

### **An appropriate response to identified offending**

40. As noted at the outset, this Union is supportive of the application and maintenance of proper standards for police in relation to their use of police data and information.
41. I question though whether in recent times, in the policing context, the pendulum has swung too far in favour of a strict enforcement approach, as opposed to a focus on training and education. In recent years we have seen a huge upsurge of police officers being both disciplined, and charged criminally, in respect of the misuse of computer resources. They have usually been charged under s408E of the *Criminal Code*. The Commission has made no secret, and no apologies, for this approach, and it is a matter upon which Mr MacSporran and I agree to differ.
42. In my view there have been examples in recent times where such charges have been unnecessary, and have involved significant "overreach" on the part of the QPS and/or CCC.
43. The offence of computer hacking was introduced into the Criminal Code in July 1997 in section 408E of the Code. In my view it was never intended to be used in the manner it has since been used. Certainly, the section was not considered to be relevant by the CJC when it performed its review into this topic in 2000. In recent years though, police have been almost the sole category of defendants charged under this section.
44. On the Union's records, as at the time of writing this statement, more than 20 police officers had been charged criminally under this Criminal Code provision in the last five years. I expect that each one of those officers then faced subsequent disciplinary action in respect of exactly the same issues. Countless more officers have been dealt with at a disciplinary level without the preceding criminal charge.

---



**IAN JOHN LEAVERS**



45. In my view, a number of the criminal prosecutions instituted have been oppressive towards the police officers involved. For example, we have seen recent (unsuccessful) prosecutions for cases involving:

- An officer providing information to a domestic violence victim to assist that victim determine if she needed to go to the police for her own protection;
- An officer charged with the aggravated offence (under s408E(2)) of receiving a benefit, simply because the mere information (knowledge) he obtained from accessing the police computer was regarded as a 'benefit';
- Instances where the prosecution concede that an initial search was authorised, but that the searches went "one screen too far" and therefore became criminal at that point.

In one current (ongoing) example, an officer has been charged for accessing his own records to create a training manual to deal with certain tasks.

46. I need to emphasise that I am not for a moment suggesting that the misuse of the police information system is not serious, or should go unpunished. Rather, I hold concerns about the fairness of the strict enforcement approach that has been adopted in recent years, particularly in light of:

- the lack of clarity in current police policy, as discussed above;
- the insufficient training for police in respect of this issue, as discussed above;
- the focus upon police in preferring criminal (as opposed to disciplinary) charges for misuse.

47. Again, I am not suggesting that criminal charges are never appropriate. An officer who is acting in a sinister way – selling information or otherwise personally profiting, or causing serious adverse consequences for others, is a proper candidate to be charged criminally. What we have seen though is a fixation on charging officers criminally in far less culpable circumstances, such as those noted above. There is also room in my view for the more judicious use of the offence provision found in s10.1 of the Police Service Administration Act – in my view if criminal proceedings are thought necessary, it should be considered before the Criminal Code offence.

48. In my view the vast bulk of cases of alleged misuse of confidential information, particularly where there is no sinister motive, can and should be dealt with as opportunities for further training and education, and in more serious cases, through the police disciplinary system. That is particularly so in light of the remedial focus for of the

---



IAN JOHN LEAVERS

## CCC EXHIBIT

new discipline system, with an emphasis on identifying and correcting inappropriate conduct early.

### Conclusion

49. The QPUE is supportive of ongoing steps being taken to ensure that police information is dealt with appropriately. In my view, the steps required to be taken in that regard include:
- the introduction of clearer and better-defined policy;
  - better training for police, and
  - a more balanced approach in considering whether a disciplinary or criminal response is required where offending is identified.
50. The QPUE remains committed to the highest standards of policing, and is prepared to work constructively with the CCC and the QPS to achieve those ends. In doing so, it is hoped that the right balance can be achieved, for the good of police officers generally, and thereby the QPS as an organisation, and the broader community it serves.

STATEMENT signed

*15th*

day of

*November*

2019.



IAN JOHN LEAVERS

20190822/D1/BSD/DC/23/Richards P/dcj

---

And you and I have talked about this issue before?---We have.

When QPRIME was first put in it was one of those things, which you can well understand for those of us who use computer systems, there was a relatively slow uptake on the use of that remarks field?---Correct.

And it's not, in fact, mandatory to put anything in there, is there?---No, it's not. It's for self-reference.

Understood. Now, if we then come back just in our heads to that task list that was there. I think they're about - - -?---Fourteen.

Fourteen. Thank you. I was going to guess 15, but we'll run with yours. Those fields, again, they're intended to put tasks into broad categories?---Correct.

And it's for the purpose of being able to effectively categories the activates that a person then undertakes?---Correct.

All right. And task admin, I would expect, is one of those ones that's pretty heavily used by police officers?---Not so much by police officers, to the best of my knowledge. How people interpret that list and how they apply it: there is a user manual that gives them guidance. Admin is normally for people, for example, our unsworn officers, performing an administrative duty in the system. So they may be cleansing some records or tidying some records up. So it's not meant to be correspondence administration or anything else like that from an officer's perspective. Some officers may interpret it that way.

That's exactly where I was going to get to. That's fine. Thank you very much. Now, in your statement that you've helpfully provided to us and which you've effectively summarised in your evidence thus far, what you do is explain, in light of your experience in the development and implementation of QPRIME, what, effectively, the rules of engagement are for people with access to that system. Is that a fair way of putting it?---You could say that.

All right. And, in particular, for the purposes of this case, do you agree with me – and we'll come to the detail in the moment – that what you do is draw a distinction between what we might call authorised use of information in QPRIME and personal use of information in QPRIME?---Correct.

Those two kinds of ideas?---Yes.

And you've identified again in your statement and in your evidence briefly today, really, two sources – I'm sure there are more, but two primary sources of those rules of access for QPRIME. The first being what you've called the standard practice?---Correct.

And, to be precise, that's the standard of practice of 2012/33?---Yes.

And then the section is what you've called, I think it's the Information Management Manual?---Correct.

5 I will refer to it, because it's referred to in this way in your statement, as the IMM. Is that the way it's commonly referred to?---Correct.

10 All right. Thank you. Now, dealing for a moment which the IMM, the Information Management Manual, you obviously – as is completely proper and normal – have confidence with the learned Crown prosecutor in advance of giving evidence in this case?---Yes.

All right. And you understand that the contents of that vary properly gets disclosed to us in the form of a memo?---Yes.

15 All right. Do you agree that the Information Management Manual is not something that mainstream police would be expected to be across?---Correct.

20 And, in fact, you wouldn't know many frontline police officers who would be aware of the IMM?---Correct.

Thank you. And the standard of practice – that standard 2012 of 33 – again, there's no – it's something which is at times sent out to police by way of sort of a group email and so on?---Correct.

25 But it's not something where there's any auditable trail or auditable requirement for use or testing on it, is there?---No.

30 No. Thank you. So in terms of access to QPRIME, we're really – in terms of a frontline officer, an officer sitting in a police station in the suburbs of Brisbane for example, on that front screen of QPRIME that we're talking about before?---So they would have that and their original training that they undertook - - -

All right?--- - - - to learn the system.

35 Now, again, just so that we can be precise, you gave us a couple of actually not bad paraphrases of the content of the relevant parts of standard of practice 2012 of 33 and the IMM in your evidence-in-chief?---Yes.

40 You obviously didn't have them in front of you?---No.

I have the benefit of your statements and quotes from those, so I just want to make sure the record is completely accurate, and I mean no criticism of your paraphrase by doing so?---No.

45 All right. The standard of practice section 16 you referred to; do you recall that?---Yes.