Access to Customer Records Policy

for Customer Services Branch (CSB)

Queensland Government

1. **Policy Status**

☐New ☒Revised ☐Rescinded

2. **Effective date**

19/08/2019

3. **Responsible Officer**

Julia Hopkins-Martin
Director, Business Management
Customer Services Branch

4. **Document control**

If you have any questions or suggestions for improvement, please contact:
Jessica Crawford
A/Snr Procedures Officer (Capability, Engagement and Learning)
Customer Services Branch

5. **Version history**

Version no.	Date	Changed by	Reason
1	30/05/2013	Andrew Musgrave	Approved
1.1	18/06/2013	Andrew Musgrave	Updated
1.2	05/02/2019	Jessica Crawford	Updated and included case studies and feedback from ESU, HR and the CSB network
1.3	16/08/2019	Julia Hopkins-Martin	Updated
2	19/08/2019	Jessica Crawford	Approved

6. **Background**

Through its legislative powers, the Department of Transport and Main Roads (TMR) gathers and stores a significant amount of personal information about individuals, organisations and other entities. The public expects that their information will only be accessed and used for the purpose that it was provided, or when required under law. As custodians of this information, Customer Services Branch (CSB) must display the highest standards of integrity to maintain public confidence and trust.

7. **Purpose**

CSB is responsible for making sure that employees meet their legal obligations relating to the privacy and confidentiality of customer records held by or available to TMR. The purpose of this policy is to provide:

- Clear instructions to all employees that they must **not** access customer records unless that access is authorised;
- The circumstances when customer records stored in a register may be accessed;
- Consequences for accessing records when that access is not authorised;
- Clear definitions.

8. **Instructions**

This policy should be read in conjunction with the **Related Policy/Legislation/Training**.

Control + Click on words that are ***bold italics*** to view their definition.

9. **Scope**

This policy applies to:

- Any **Customer records**;
- All **Employees**;
- Managers, who must ensure that staff:
  - Are only granted profiles according to the role they hold and
  - Read this policy and complete the ***Training***.

10. Definitions

(a) Customer records

Private and/or confidential details that are obtained, used by or available to TMR under legislation and are stored in a register, paper or electronically. This includes online services.

(b) Access

Entering, reading, editing, printing, copying, retrieving, manipulating, searching or otherwise using or supplying information in customer records available to an employee through:

- Internal or remote login to the TMR network;
- Computer/device download or other technology such as a memory storage device;
- TMR online services

(c) Authorised access

Is accessing a record when:

- There is a genuine "need to know" and the information is being used as part of the employee's official duties and they would be hindered in their performance if they didn't access the information;
- The employee is entitled to access the information under law;
- A customer has given permission for their login details to be used to access online services - this is for the customer contact centre/Help Direct/Online Support/Ebus/CAM only following completion of verbal EOI;
- There is an official business transaction to be completed, including a transaction for a work colleague. The official business transaction must be done over the counter or via the call centre and the employee treated the same as any other customer (e.g. a ticket must be taken, full transaction requirements must be met).
  A SASM/Manager must also be informed to remove any perceived or potential conflict.

(d) Unauthorised access

Is:

- Accessing your own customer record;
- Accessing customer records of friends or relatives (even if they have given permission) including online services if using a work computer;
- Accessing a record where an actual, perceived or potential conflict of interest exists;
- Accessing information because it would be convenient for a staff member to know;
- Accessing a record on behalf of another TMR employee unless it is part of an official business transaction (e.g. contacting help direct or asking a colleague to access a record to assist with a transaction **is** acceptable);
- Assisting a third party to access a customer's record (e.g. mother calls and asks about an issue her family member is having with an online service and the employee assists the mother using the family member's details).

(e) Conflict of interest

A situation where your personal or private interests could, or be seen to improperly influence the performance of your official duties or the responsibilities of TMR:

- *Actual conflict* – direct conflict between your official duties and competing interest or obligation whether personal or involving a third party;
- *Perceived conflict* – where it could reasonably be perceived, or give the appearance, that a competing interest could improperly influence the performance of your official duties and TMR's responsibilities;
- *Potential conflict* – where you have an interest or obligation, whether personal or involving a third party that could conflict with your official duties and TMR's responsibilities.

(f) Customer

Is an individual, organisation or other entity that:

- Conducts business with TMR; and
- Has been allocated a customer reference number; and
- Has been created as an entity in a register.

(g) Register

Is a TMR database where customer entities and related personal information are created, actioned and stored such as the Transport Integrated Customer Access (TICA), Transport Registration and Integrated Licensing System (TRAILS) or the TMR website (online services).

(h) Employee

Is a person engaged by CSB including:

- All ongoing employees;
- Non-ongoing employees (e.g. persons now working for other TMR division);
- Persons who provide services for the division (e.g. casual staff, contractors, consultants);
- External agency staff that provide CSB services for the department (e.g. QPS, Smart Service Queensland);
- Any other person appointed or engaged by CSB to perform the duties or functions of the branch;
- An employee other than an employee defined above engaged by TMR (e.g contractors and other people who provide services for the department).

(i) Authorised employee

- Is an employee granted authorisation to access a **Register**; and
- Must maintain a clear desk (keep paper customer records safe/secure) and clear screen (keep computer locked) when absent from their desk.

(j) Profile/authorisation

- The system profile access approved by a supervisor or manager for an employee based on the position they hold which they use to access customer records stored in a register;
- Is only allowed to be issued to an employee for one position at a time;
- Must be reassessed (to see if it's still applicable) when employee's role within TMR changes;
- Must be withdrawn when the duties of the position the employee holds within the organisation no longer requires the ability to access records for work;
- May be withdrawn as a result of Criminal History screening results;
- Must be maintained according to the procedures outlined in DocBase.

(k) **Authentication/login** – a unique user id and a password (which is strictly confidential) that is:

- Created to meet corporate security requirements;
- Used by the employee to access registers through the TMR network;
- Not to be given to or used by anyone else.

(l) **Privacy** – the way that the department must manage the personal information it holds according to the *Information Privacy Act 2009.*

11. Policy Statement

Accessing customer records:

- An **Employee** must not perform any **Unauthorised access** to **Customer records**;
- An employee must only complete **Authorised access** to customer records;
- A **Customer** cannot authorise an employee to override the conditions of this policy;
- An employee must not access customer records**Customer records** to confirm whether a customer**Customer** is complying with their legislative obligations, unless specifically required by the duties that the employee is currently performing. If the employee suspects the customer is not complying but is not authorised to act on that suspicion, they must refer the matter to their immediate supervisor for investigation;
- Employee access to customer records will be managed via manual and electronic monitoring including:
    - Electronic reports which shows user **Profile/authorisation** activity (all records accessed including their own CRN), trends and unusual transactions
    - Manager/Quality Assurance Officer observations
    - Internal and External Audits

Compliance:

- Employee compliance with this policy will be managed via manual and electronic monitoring including:
    - Electronic reports which show user **Profile/authorisation** activity (including records accessed including own CRN)
    - Other electronic intelligence that identifies trends and unusual behaviours;
    - Manager/Quality Assurance Officer observations including checking of filing reports
    - Internal and External Audits
- This policy does not override or supersede statutory provisions related to the use and disclosure of personal information or corporate policy
- In complying with this policy, an employee must abide by all **Related Policy/Legislation/Training**.

Consequences:

As outlined in the **Appendix A**

Case studies, any breach of privacy (even a "peek") can have serious consequences including:

- Termination of employment;
- Reduction of classification level and a consequential change of duties;
- Transfer or redeployment to other public service employment;
- Forfeiture or deferment of a remuneration increment or increase;
- Reduction of remuneration (increment) level;
- A monetary penalty (which can be deducted from your pay);
- A formal reprimand;
- Criminal prosecution and/or action under the *Public Service Act 2008* as outlined in Chapter 6 - Disciplinary action for public service officers and former public service officers.
- Suspension from duties;
- Record of disciplinary action - permanent record of the incident on their file which they would need to disclose during pre-employment screening for all public sector roles;
- Reputation damage and loss of trust;
- Stress - an overall impact on your own and family's health and wellbeing.

Responsibilities:

Manager, (Capability, Engagement and Learning) is responsible for:

- Reviewing and maintaining this policy;
- Communicating the policy and procedures to the key stakeholders;
- Displaying the policy on the CSB Homepage;
- Inclusion of this policy in CSB training programs.

All Managers and supervisors who have employees with access to customer records must ensure:

- Every ***Employee*** they are responsible for is aware of this policy;
- Compliance with this policy including:
    - Adapting TRAILS ***Employee Authorisation*** procedures to suit the work environment (e.g. in a solo site may be set up may be different to a large centre);
    - Not knowingly, willingly or intentionally causing or asking an employee to breach the policy;
    - Regularly monitoring employee adherence to the policy at an individual and office/business area level;
    - Actively engaging with employees to reaffirm their responsibilities under the policy;
    - Proactively managing suspected non-compliance of the policy;
    - Immediately bringing suspected breaches of the policy to the attention of their superior.
- That their employees:
    - **Profile/authorisation** is current, updated and removed according to the ***Employee Authorisation*** procedures;
    - Have completed all mandatory Accelerate training.

Employees are responsible for complying with this policy including:

- Not knowingly, willingly or intentionally causing or asking another employee to breach the policy;
- Actively seeking advice from their immediate manager or supervisor in situations where they are unsure whether the access of a customer record would constitute an **Unauthorised access**;
- Complete and understand all mandatory training, seeking advice from their supervisor if any content is unclear;
- Immediately bringing suspected breaches of the policy to the attention of their manager or supervisor, local HR and the Ethical Standards Unit (ESU).

12. Procedures

(a) *Employee Authorisation*

Procedures relating to TRAILS/TICA authorisation are contained in the DocBase Maintain Operators Guide (1293).

(b) *Suspected Breaches*

In all cases where an employee suspects that someone has breached this policy, the code of conduct, or any of the **Related Policy/Legislation**, they must immediately report it to their supervisor, manager, local HR or the ESU for

assessment, technical support or training. Failure to report a suspected breach, if substantiated, may result in disciplinary action.

(c) *Alleged Breaches*

Supervisors and Managers must ensure all allegations of failure to comply with this policy and or allegations of misuse of TMR information are reported to the ESU for assessment as to whether the alleged breach constitutes suspected corrupt conduct pursuant to the *Crime and Corruption Act 2001*. The Crime and Corruption Commission's publication titled "Prevention in Focus – Improper access to public sector databases" provides useful information regarding information misuse and strongly reinforces that information misuse is a breach of section 408(E) (1) of the Criminal Code Act 1899 - computer hacking and misuse.

Supervisors and Managers must fulfil their obligations according to the code of conduct for the Queensland Public Service and ensure that all breaches are to be dealt with according to HR Policy and Procedures for Discipline. The privacy breach response plan as outlined in DocBase must also be followed if required.

13. Related Policy/Legislation/Training

(a) Policy

Code of Conduct

Information Security Policy

Use of ICT Facilities and Devices Policy

Records Management Policy

Right to Information Policy

Complaints Management Policy

TMR Integrity Framework

TMR Fraud & Corruption Framework Organisational Policy

(b) Training

CSB staff responsibilities training (mandatory for all CSB staff)

SASM Program – Security for SASM's (mandatory for all CSB SASMs)

NETS onboarding (mandatory for all new CSC employees)

(c) Legislation

Public Service Act 2008

Public Sector Ethics Act 1994

Right To Information Act 2009

Information Privacy Act 2009

Transport Operations (Road Use Management – Vehicle Registration) Regulation 2010 - ss. 67-68B

Transport Operations (Road Use Management) Act 1995 Sections 77 and 77A

Crime and Misconduct Commission Act 2001

Whistleblowers Protection Act 1994

Criminal Code Act 1899

Evidence Act 1977 and Regulations 1993

14. Privacy complaints

Written or verbal complaints received by employees from a customer, employee or other stakeholders about how the department has dealt with their personal information are to be promptly referred to the Privacy Contact Officer.

Any documents received regarding a privacy complaint or enquiry are to be emailed and the originals of the documents forwarded to:

The Privacy Contact Officer,

RTI, Privacy and Complaints Management

Department of Transport and Main Roads

Phone 3066 7568

Email: privacy@tmr.qd.gov.au

15. Review

Review must occur every 3 years from latest approval date.

Document review indicators will be that the contents are current and accurate.

Policy review indicators and measures (as outlined below)

Indicator	Measure	Data/Source
Incidence of allegations of breaches of	Number of allegations	Internal Audit

policy		
Substantiated incidences of breaches of this policy	Number of allegations substantiated	Internal Audit

16. **Appendices**

Appendix A

Case studies

Unauthorised access of someone else's personal information is a serious matter. Even a simple peek is an unlawful invasion of privacy. These are recent real examples of when CSB employees have breached this policy, been subject to the stress and embarrassment of an investigation and then suffered serious consequences for their actions.

1.

Background:
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 TMR's TRAILS system) and asked them to access the customer's record using the registration number. The registered operator's details, including their phone number were passed onto the TMR employee who then threatened and intimidated the member of the public.

Action taken:
The member of the public took the threats to the Queensland Police Service who commenced an investigation. Information gathered by the Queensland Police Services was provided to the TMR Ethical Standards Unit for further action.

An ESU investigation was commenced and the TMR employee was removed from their substantive duties and placed on restricted duties whilst the investigation was completed.

The investigation concluded that all allegations against the TMR employee who accessed the TRAILS system and shared customer information were verified. The General Manager (decision-maker) then commenced a disciplinary process and a Notice to Show Cause was issued.

Consequences:
Stress – to the officer and family's wellbeing during the investigation/interview process;

A formal reprimand by the General Manager;

Record of disciplinary action - permanent record of the incident on their file which they would need to disclose during pre-employment screening for all public sector roles;

Reduction of increment for a period of 12 months;

Financial – loss of wages from increment reduction;

Reputation – damage and loss of trust.

2.
Background:
A TMR Customer Service Centre officer observed a colleague accessing TICA and viewing infringement notices for a customer with the same surname. Believing the TMR Customer Service Centre officer was viewing records belonging to the officer's daughter, the work colleague escalated the matter to the manager.

Action taken:
The matter was referred to the ESU for assessment. ESU determined that the matter met the criteria for referral to the Crime and Corruption Commission (CCC). The CCC advised the department that, if proven, the alleged conduct would amount to corrupt conduct.
An ESU investigation was commenced and the allegation of inappropriately accessing a customer record was verified.
The General Manager commenced a disciplinary process and a Notice to Show Cause letter was issued.

Consequences:

Stress – to the officer and family's wellbeing during the investigation/interview process;

A formal reprimand by the General Manager;

Record of disciplinary action - permanent record of the incident on their file which they would need to disclose during pre-employment screening for all public sector roles;

Reputation – damage and loss of trust.

3.

Background:
A TMR employee was engaged with a criminal organisation and was fraudulently completing transactions (issuing/upgrading driver licences, registering vehicles) and accessing customer records in exchange for money. The employee also approached colleagues and attempted to bribe them to do the same, which they declined but failed to report.

Business Exceptions had been incorrectly authorised (without being checked), which allowed the fraudulent activities to continue for 18 months undetected. It wasn't until another staff member reported the employee for looking up customer details inappropriately that the other breaches were uncovered.

Action taken:

The matter was referred to the ES and Queensland Police Service for investigation. Criminal charges were laid by the Police and the matter was heard in the Southport Magistrates Court. The TMR officer was found guilty in court.

Consequences:

Termination of employment;

Stress – to the officer and family's wellbeing during the investigation/interview/court process;

Financial – the cost of legal representation during the court process and loss of wages;

Reputation - damage and loss of trust;

Criminal prosecution/record;

Imprisonment;

Line management subject to stressful investigation process and potential disciplinary action regarding lack of due process.