CCC EXHIBIT

[redacted]

**From:** [redacted] **On Behalf Of** Geoffrey J Magoffin
**Sent:** Friday, 26 May 2017 9:22 AM
**To:** CSB.STAFF
**Cc:** [redacted]
**Subject:** Personal information: even a simple peek is a breach!

## A Message from Geoff Magoffin
**General Manager (Customer Services Branch)**

Hi everyone

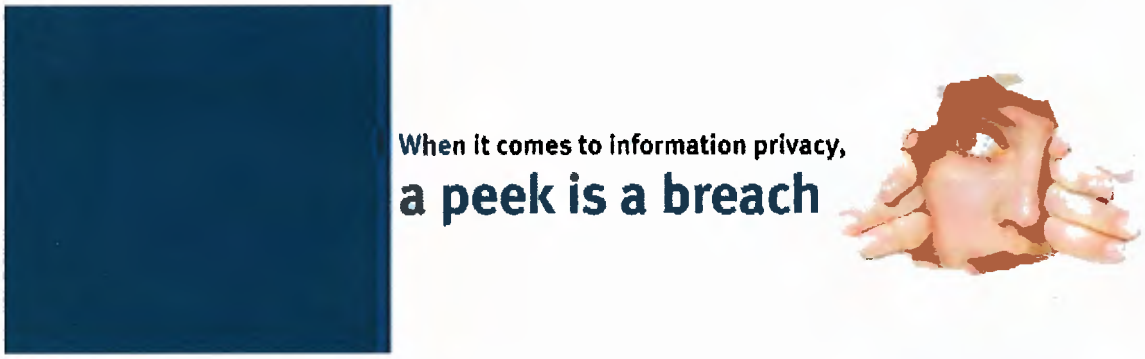
Many of us, particularly our customer-facing staff, deal with personal information on a daily basis as part of our job.

We all have an obligation to make sure our customers' personal information remains safe and secure and we only access their information to assist in customer service delivery. It also means we must not disclose their personal information without consent or falsify records.

While the majority of our staff are doing the right thing, we are aware that a small number of staff have accessed customer's personal information without a legitimate reason.

Every time you log in to our systems such as TICA and TRAILS, you are acknowledging that you will only access information necessary to enable you to undertake the specific duties assigned to you.

**Unauthorised access of someone else's personal information is a very serious matter. Even just a simple peek at some else's personal information is a breach of the TMR Code of Conduct and is an unlawful invasion of privacy.**




Accessing personal information without authorisation may not only result in disciplinary action from TMR including termination of employment, but also a criminal conviction. TMR can also be prosecuted if an employee breaches the privacy act for failing to adequately safeguard information.

However, sometimes the consequences don't end there. You need to think beyond your own actions and to how they could affect the customer or people close to them. Managing a breach is bigger than just managing the employee's action. TMR has a legal obligation to manage the consequences of the breach as it may have the potential to impact on a customer's circumstance and safety, and damage TMR's reputation as the custodians of private information. TMR has an obligation to report breaches to affected members of the public and manage their expectations in relation to re-establishing security on that information.

We monitor and record system activity, so if you do the wrong thing you will be caught. If you have access to TICA or TRAILS systems you need to complete the CSD Staff Responsibilities training on Accelerate (formally Learnzone) annually.

If you suspect a colleague has acted inappropriately regarding information privacy, you should notify your line manager or TMR's Ethical Standards Unit. The Public Interest Disclosure act protects people who speak out about wrongdoing when there is genuine concern.

CSB's Accessing Customer Records policy on InsideCSB explains what is considered to be authorised and unauthorised access to customer records. I strongly encourage you to revisit the policy and refresh your understanding of these requirements and discuss them at your next team meeting.

Regards
Geoff

**Geoff Magoffin**
General Manager | Customer Services, Safety and Regulation Division
**Customer Services Branch** | Department of Transport and Main Roads