

Dealing with a personal information breach

Dealing with a personal information breach

Personal information security breaches relating to our customers or employees can occur for a number of reasons, including:

- Human error resulting in accidental disclosure of personal information (leaks)
- Our employees or service providers being deceived to give personal information (blagging)
- Media with personal information, such as laptops or paper files, being lost or stolen
- Personal information being maliciously disclosed (leaked) by current or ex-employees
- Access controls for IT systems and premises being inadequate or inappropriate
- 'Hacking' or other forms of attack against our IT infrastructure
- Unforeseen circumstances such as IT equipment failure, fire or flood

You must tell your supervisor or line manager immediately if you suspect a security breach involving personal information,

You must also report it to the Cyber Security and Incident Response Team (CSIRT) as quickly as possible, by emailing [REDACTED] or by calling [REDACTED]

Investigating a breach

If the security breach is classed as a serious incident, an incident management team will be formed including representatives from the relevant business areas. The team will manage and resolve the security breach, providing a centralised point of contact for a co-ordinated response.

The incident management team will:

- Minimise TfL's exposure and mitigate risk by carrying out a rapid assessment of the impact of the incident
- Assess any ongoing risks for TfL and for individuals affected, recommending remedial action to minimise re-occurrence of the breach
- Decide who needs to be notified of the breach, considering the potential harm to those affected by the breach, (this could include the police and/or the Information Commissioner's Office)
- Evaluate what went wrong and implement any necessary changes to business processes

