Transport for London

Dealing with a personal information breach

All concerned

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 out personal information (blagging)
- Media containing personal information, such as laptops or paper files, being lost or stolen
- Personal information being disclosed maliciously (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

This form is for you to give feedback on how this page is written and what information is included. If this information affects you personally and you need advice, use the contact details above where provided.

You must tell your supervisor or line manager immediately if you suspect a security breach involving personal information. By law personal data breaches must be reported to the regulator within 72 hours of discovery, so the Privacy team need to be told straight away, even if you haven't managed to establish all the facts at that point.

You must also report any security breach to the Cyber Security and Incident Response Team (CSIRT) as quickly as possible, by emailing cybersec@tfl.gov.uk or by calling 020 7027 9260 (auto 59260).

.

Content last updated: 21 May 2018 13:12

For questions about the Tfl management system ask the One Tfl Management System Project

nvestigating a breach

f 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, as well as the individuals whose data has been affected)
- Evaluate what went wrong and implement any necessary changes to business processes