

T R Davies Ltd

Data Breach Policy

1. When there is a personal data breach, the ICO advises:

Tell it all. Tell it fast. Tell the truth.

2. The designated data protection lead (Tim Davies) is responsible for handling personal data breaches. In particular he will evaluate what the breach is and how it occurred, and the associated risk to data subjects and T R Davies Ltd.
3. If there is a risk to data subjects, the breach will be reported to the Information Commissioners Office in 72 hours. T R Davies will report to the ICO how the breach occurred, what steps are being taken to reduce the risk, and how a similar breach is to be avoided in future.
4. Where the risk to data subjects is high, the breach must be reported to them individually if at all possible. If there is a large number of data subjects at risk, it may not be logistically possible to do so, in which case a notification provided on T R Davies Ltd's website.
5. A thorough investigation and corrective action will be necessary so as to reduce the risks to data subjects arising out of any breach, and to make sure that something similar does not happen again in future.
6. Where a breach of T R Davies Ltd's computer systems is suspected, the data protection lead will engage the support of T R Davies Ltd's IT provider in order to identify the nature of any breach of T R Davies Ltd's computer systems.
7. The theft of data, whether as a result of shortcomings in the physical security arrangements on the premises, or the hacking and penetration of computer systems, or theft by a member of staff, will be reported immediately to the police.
8. The breach, investigation and corrective actions will be documented and filed on the data protection risk register. So, too, will the report made to the ICO.
9. All personal data breaches, however minor, and whether reportable or not, are recorded in the data protection risk register, held by the data protection lead.