# DATA PROTECTION BREACH REPORTING PROCEDURE

As a business, we are responsible for ensuring that personal data processed by the business is not:

- Accessed without authority;
- Processed unlawfully;
- Lost;
- Destroyed; or
- Damaged.

Nevertheless, we realise that from time-to-time things may go wrong and we might fail to achieve one or more of our data protection responsibilities.

If this does happen, it is essential that we take steps to try and put things right. However, we can only do this if we know that there has been a problem.

Therefore, everybody in this business has a duty to report any actual or suspected data breaches, regardless of whether they have discovered them or have caused them.

## WHAT IS A DATA PROTECTION BREACH?

A data protection breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Data protection breaches can happen for a wide range of reasons, including:

- Human error;
- Cyber-attacks;
- Loss or theft of devices or equipment on which personal data is stored;
- Inadequate or inappropriate access controls;
- Deceit; and
- Disasters at business premises i.e. fire or flood.

If you are unsure whether a particular circumstance or incident constitutes a data protection breach, please refer the matter to your line manager or another appropriate manager in their absence for guidance.

## REPORTING A PERSONAL DATA BREACH

All personal data breaches must be reported to Calteq's DPO Nigel Willetts immediately upon discovery.

Reports should be made by secure email to dpo@calteq.co.uk