# 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 is responsible for handling personal data breaches. In particular he or she evaluates what the breach is and how it occurred, and the associated risk to data subjects and QMLS

3. If there is a risk to data subjects, the breach must be reported to the Information Commissioners Office in 72 hours. If the report is late, an explanation must be given as to why.

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 press release should be given and notification provided on QMLS's website.

5. Encryption of personal data is likely significantly to reduce the risk to data subjects following a breach, and QMLS encrypts high risk personal data such as identification records and medical and health records.

6. The ICO will want to know how the breach occurred, what steps are being taken to reduce the risk, and how a similar breach is to be avoided in future. The initial report need contain no more than a summary of the position. The data protection lead or The Director may wish to seek authority to obtain legal advice before submitting the initial and any subsequent reports.

7. A thorough investigation and corrective action are 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.

8. Where a breach of The Director's computer systems is suspected, the data protection lead will wish to engage the support of The Director's IT provider in order to identify the nature of any breach of The Director's computer systems.

9. The Director has obtained cyber security insurance and any IT related breaches must be reported to insurers immediately. They may provide affected data subjects with free access to security measures to protect their identity.

10. 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, should be reported immediately to the police.

11. The breach, investigation and corrective actions must be documented and filed on the data protection risk register. So, too, should the report made to the ICO.

12. All personal data breaches, however minor, and whether reportable or not, such as non-compliance with The Director's clear desk policy, are recorded in the data protection risk register, held by the data protection lead.