

# Data Security Policy

1. This security policy is designed to ensure that QMLS complies with the security requirements of the General Data Protection Regulation, and the rights to privacy of data subjects are protected.
2. In compliance with Article 32, QMLS has implemented appropriate physical, organisational and technical measures to ensure a level of security appropriate to the risk.
3. QMLS is at D202 Dean Clough Mills, Halifax, HX3 5AX

## Security measures

4. The following security measures have been taken:

### Physical

- Office building is alarmed/protected by CCTV cameras;
- Visitors to premises are supervised at all times;
- Areas of the premises where personal data are kept are secured by locks/complex security codes;
- Computer screens are arranged so they cannot be viewed by casual passersby, particularly visitors;
- Hard copy material containing personal data is stored securely and locked away in fire proof;
- Filing cabinets at night;
- A clear desk policy is enforced;
- Hard copy special category data, such as medical records, are kept separately from other;
- Personal data in locked and fire proof cabinets with restricted access;
- Electronic special category data is encrypted with restricted access;
- Passports, driving licenses and any other documents used to check identity are also kept separately, stored securely with restricted access. When stored electronically, the information is encrypted with restricted access;
- Electronic data is backed up off site;
- Any server on the premises is kept in a locked room;



- Shredding of confidential information is carried out securely on site or outsourced pursuant to a GDPR compliant contract;
- Mobile equipment such as laptops are encrypted and locked away when not in use. There is a system in place for issuing them to staff working off site;
- Staff working off site must follow guidelines on the printing and disposal of hard copy material;
- Computers and other electronic equipment are disposed of in a safe manner by an outsourced and certificated provider.

#### 5. **Managerial**

- This policy is regularly reviewed and the Director is committed to ensuring it is implemented.
- The Director is responsible for data protection and has powers to discipline for breaches of this and other data protection policies;
- The Director has sufficient resources to carry out its role effectively as data protection lead;
- Staff compliance with this policy is monitored by file handling audits and spot checks;
- Staff are trained in data protection;
- Only designated staff may delete data and they receive specific training in this regard;
- Breach of this security policy is a disciplinary offence;
- There is in place a procedure for authenticating the identity of telephone callers, clients and contractors;

#### 6. **Technical measures**

- Anti-virus and anti-spyware tools are installed on all computers;
- All computers are encrypted and password protected;
- It is a disciplinary offence to share a password;
- Computers are programmed to download patches automatically;
- Computers have automatic locking mechanisms when not in use;
- Staff are prevented from downloading software from the internet onto work computers and laptops;
- They cannot transfer data onto removable devices such as USB sticks and CDs without the authority of The Director;



- Staff are encouraged to save personal data on their computers in a consistent manner;
  - They have access rights to personal data on a strict need to know basis;
  - Access rights are monitored and reviewed. They are deleted when a member of staff leaves;
  - Staff are forbidden to use their personal email addresses for work;
  - Computers, laptops, mobile phones, USB sticks and CDs are encrypted and password protected;
  - Personal data is encrypted before it is uploaded onto the cloud;
  - Personal data shared by email are encrypted and password protected as appropriate.
7. Security measures are tested and evaluated once a year.
  8. Whenever a new project, process or procedure is introduced which carries a high risk to data subjects, a Data Protection Impact Assessment is carried out, at the instigation of The Director.