

DATA PROTECTION

MATTERS2ME CIC



Policy: Data Protection policy

Policy Statement

Matters2Me CIC will fulfil its obligations under the **Data Protection Act 2018**.

Procedure

Employees must observe the provisions laid down in the Data Protection Act 2018. Matters2Me CIC will provide any information and training necessary to comply with the legislation. However, it is every employee's responsibility to ensure that they fully understand the terms of the legislation. The main points are detailed below.

The Act is concerned with the processing of information about living individuals (personal data) and gives rights to the individuals who are the subject of that information. It places certain obligations on the Organisation's data user; in respect of the personal information it processes or causes to be processed on its behalf by third parties. The Act applies to computerised and manual filing systems.

The aims of the Act are embodied in the eight Data Protection Principles. Anyone processing personal data must comply with the eight enforceable principles of good practice. The principles state that data must be:

- Fairly and lawfully processed.
- Obtained for specified purposes and not processed in a manner incompatible with those purposes.
- Adequate, relevant and not excessive for the purposes for which it is processed.
- Accurate and kept up to date.
- Not kept for longer than necessary for the purposes.
- Secure.
- Not transferred to countries without adequate protection.
- Processed in accordance with the data subject's rights.

It is important that all employees are aware of the existence of this Act and the principles on which it is based. In particular, they must not access or disclose any personal data other than is necessary to carry out the role for which they are employed.

If an employee requires any guidance on their obligations under the Act, the employee should consult their manager.

If an employee discloses personal data in breach of the principles set out in the Act, such disclosure may result in the commission of a criminal offence. It could also lead to disciplinary action being taken against the employee.

Physical Security of Data Files

Paper files, physical drives or removable media containing personal data must be stored in lockable cabinets or secure rooms when not in use.

Digital Encryption of Data Files

Electronic files with highly sensitive personal data will be managed using CPOMS or password-protected/encrypted, with 2-factor verification to prevent unauthorised access.

Access Control of Data Files

Files are 'locked' by permission levels (access controls) so that only staff who have a strict business need (e.g. HR or Payroll) can view or modify them.

Automatic Session Locks

Devices (laptops and desktops) accessing these files require screen locks and password re-entry after short periods of inactivity.

The rights of individuals to access personal data

The Act provides enhanced rights to individuals to access personal data stored about them. Employees are allowed to have access to personal data held by Matters2Me CIC if needed to complete their role. If an employee wishes to access their personal data, the employee should consult their manager. The manager will provide guidance to the employee to enable them at reasonable intervals to access their personal data.

Date policy adopted: _____

Signature of Chair: _____

Date policy to be reviewed: _____