

General Data Protection Regulation: Security Policy

This security policy is designed to ensure that Morris & Co (Handlers) Ltd complies with the security requirements of the General Data Protection Regulation (GDPR), and the rights to privacy of data subjects are protected.

1. In compliance with Article 32, the company has implemented appropriate physical, organisational and technical measures to ensure a level of security appropriate to the risk.
2. The company is based at Bankwood Lane Industrial Estate, Rossington, Doncaster, DN11 0PS. The company also has 3 further sites in the UK.

The premises can be described as: Metal Recycling Site.

3. Physical security measures:

- 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 that they cannot be viewed by casual passers-by, particularly visitors.
- Hard copy material containing personal data is stored securely and locked away in fire proof filing cabinets at night.
- Hard copy special category data, such as medical records, are kept separately from other personal data in locked and fire proof filing cabinets, with restricted access.
- Where this information is stored electronically, it 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. Where 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.

4. Managerial security measures:

- This policy is regularly reviewed, and senior management is committed to ensuring it is implemented.
- The Management are responsible for data protection.
- The Management has powers to discipline staff for breaches of this and other data protection policies.
- Staff are trained in data protection.
- Only designated staff may delete data and they receive specific training in this regard.
- There is a procedure in place for authenticating the identity of telephone callers, customers and contractors engaged by the company.

5. Technical security 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.
- They cannot transfer data onto removable devices such as USB sticks and CDs without the authority of the Management.
- USB sticks and CDs used to transfer information are encrypted.

- 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 without their written permission.
 - Personal data are encrypted before uploading onto the cloud.
 - Personal data shared by email are encrypted and password protected as appropriate.
6. Security measures are reviewed, tested and evaluated at least once a year.
7. Whenever a new project, process or procedure is introduced that carries a high risk to data subjects, a Data Protection Impact Assessment is carried out, at the instigation of the Management.