PURPOSE:

1. This policy provides details of how we handle and manage information to ensure its security, and what must be done when communicating information via email or by the use of any removable media device.

INTRODUCTION:

2. Ensure everyone handling and managing personal information is appropriately trained. There are different types of information that are handled in specific ways. Content consideration must be given to determine the level of protection with regards to confidentiality and security as to how it should be handled and stored.
   This applies to both physical paper copies and electronic copies.
   This policy applies to all staff; each employee with access to information has an individual responsibility to ensure compliance with our procedures failure to comply could result in disciplinary action.

ELECTRONIC DATA/REMOVABLE MEDIA

3. Anti-virus and firewall protection is installed to ensure protection off data from malicious damage. Where electronic system documents are made available to staff on the network check it is adequately read/write protected to ensure control over content is maintained. It must be protected from unauthorised access and accidental deletion.
   All electronic data is backed up to a remote PC in a secure location.
   - All removable media must be virus-checked on the stand-alone PC before using on the network.
   - Any removable media containing company information must be kept as secure as the equivalent paper documents.
   - Personal removable media must **not** be used.
   - All must be adequately protected.

RETENTION/DISPOSAL OF INFORMATION

- Information must be retained for the agreed retention schedules.
- Delete or dispose of securely when no longer needed.

PAPER DATA STORAGE

4. This policy also applies to data that is usually stored electronically but has been printed out for some reason.
   - Paper documents or files should be kept locked in the filing cabinet, they must not be left where unauthorised people could see them.
   - Data printouts should be shredded and disposed of securely when no longer required.

SENDING DOCUMENTS BY EMAIL

5. We use the Egress software, which enables us to send and receive encrypted information.
   Confidential and sensitive information should not be sent via email unless the appropriate confidentiality and security procedures are used. The recipient email address must be checked.

RELEVANT LEGISLATION

6. We will comply with all legislation and statutory requirements relevant to information and information systems, including, but not limited to:

    - Computer Misuse Act 1990
    - Data Protection Act 1998
    - General Data Protection Regulations 2018 (GDPR)
    - Environmental Information Regulations 2004

CCTV

7. CCTV is used for maintaining the security of property and premises and for preventing and investigating crime. It may also be used to monitor staff when carrying out work duties. For these reasons, the information processed may include visual images, personal appearance and behaviours. This information may be about customers, staff and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where necessary, or required, this information is shared with the data subjects themselves, employees and agents, service providers, police forces, security organisations and appropriate persons making an enquiry.

SHARING INFORMATION

8. Where necessary, we share certain personal information with:

    - Licensing authorities
    - Occupational health providers
    - Principal Contractors of Highways projects
    - Training providers in conjunction with licensing and qualifications
    - Government bodies in conjunction with the reporting of certain accidents/injuries (HSE)

9. We will only use personal information where we are allowed to by law, fulfilling a legal obligation, because we have a legitimate business interest or where you agree to it. Information is never sold on to third parties.

10. Any data breaches or 'hacking' will be thoroughly investigated.

11. Roocroft RRS will remain within data protection compliance.