Summary / Background

Kier's policy is to secure and use confidential information and IT systems in a manner that complies with applicable legislation and which meets accepted industry practice protecting information from unauthorised use, disclosure or destruction.

What is the requirement?

All Kier employees as well as those who have access to Kier IT systems and confidential information are required to be familiar with the standards set out in this policy and the Information Security standard and comply with the requirements contained within them. In respect of confidential information, users are required to understand the confidentiality obligations when handling such information and process the information in line with those obligations. In relation to information governed by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (together DP Legislation) users are required to understand and comply with the DP Legislation principles.

Why is it important?

By implementing appropriate controls, we will ensure the continuity of our business operations and mitigate business impact in the event of a security incident. Kier's activities are critically dependent on the information and information systems that underpin its business operations. The consequences of a breakdown of our controls can have a significant impact on its operations.

In respect of information governed by DP Legislation, we are required to comply with the law and, as custodians of personal data, we have responsibilities regarding its secure and proper handling. It is important from a legislative perspective and also as a responsible and trusted organisation that personal data is processed appropriately and in compliance with the law. The consequences of breaching the law can be severe.

What must I do / not do?

Each of us have responsibilities regarding safe and appropriate handling of IT systems. These are as follows:

- Kier's Chief Information Officer (CIO) has oversight of information risk management within Kier Group and owns this policy on behalf of the Executive Directors.
- The CIO is specifically responsible for:
- developing and implementing business appropriate information risk management processes that are aligned with and support the requirements and principles of this policy;
- developing, promoting and facilitating the implementation of a set of risk specific Information Security and IT technical standards that are aligned with and support the requirements and principles of this policy; and
- ensuring Kier's IT infrastructure is designed, procured, configured, maintained and operated in compliance with these policy requirements.
- Kier's Data Protection Officer (DPO) is responsible for ensuring compliance with the DP Legislation.
- Kier's Group Managing Directors are responsible for ensuring that Kier's business operations are compliant with these policies.
- Finance Directors (or their equivalent) are responsible for maintaining ICO registration for the Business Unit in conjunction with the Company Secretarial team.
- Line managers are responsible for ensuring employees are aware of Kier's Information policy and standards and have the necessary skills to operate them.
- All Kier employees must comply with all Kier information security standards, and to highlight any areas of non-compliance to their management.

Kier treats its information, as well as those who Kier holds information on behalf of, such as its clients and customers, as an important asset. IT assets and confidential information will be:

- treated as an important corporate resource;
- subject to Kier's applicable Policies and Standards;
- managed such that associated risks are known and is within Kier's risk appetite or relevant tolerance levels
- protected in a manner proportionate to its sensitivity following an assessment to determining the level of control required against the risk to Kier and its stakeholders, as mentioned in Kiers protective marking standard;
- protected from loss of confidentiality, loss of integrity and loss of availability;
- available only to users who need access and limited to the information which is necessary;
- monitored to identify actual or potential breaches of this policy;
- subject to a security process of continual review and improvement; and
- managed and secured such that all relevant regulatory, legislative and contractual requirements are met.
- You must:
- comply with this policy;
- be appropriately trained in the handling of confidential information and use of Kier IT;
- with regard to personal data processing, comply with the six data protection principles. Personal data must be:
  - processed fairly, lawfully and in a transparent manner;
  - processed for a specified purpose;
  - minimised;
  - accurate;
  - not kept longer than necessary; and
  - processed securely;
- process personal data in a manner that will enable Kier to demonstrate accountability in meeting each of the six principles
- seek Group Compliance approval where personal data is transferred outside the UK;
- only share personal data on a 'need to know' basis and only share in a secure manner;
- maintain records of data processing;
- complete a Data Privacy Impact Assessment when commencing a new project, or making material changes to an existing project or otherwise, where there is a potential change to the privacy risk profile and where in each case the project involves personal data processing (for example when installing CCTV or using drones (see Information Security standards for more information on each);
- process personal data in accordance with Data Subject's rights;
- report personal data breaches to the Group Data Protection Officer (DPO), David Foster (compliance@kier.co.uk) immediately after becoming aware of any data incident. In no circumstances should you communicate details of the incident outside of those managing the data security incident without first contacting the DPO; and
- report all other breaches of information security, whether actual or suspected, in accordance with Kier's Major Incident Response Plan and associated procedures.

This policy should be read in conjunction with the Chief Executive Foreword, Information Security Standard, Information Technology Standard, the Group's Protective Marking Guidance and the Document Retention Policy.