# Section E – Data Management & Protection Policy

## 1. Introduction

Kelda Group aims to manage data to a standard that protects the reputation of the organisation and enables value to be delivered to customers, stakeholders and investors.

This Policy summarises what is expected of Group directors and employees in their handling of data, which ensures compliance with: legislation, regulation and Company standards.

The Policy is applicable to employees and directors of the Group.

The Policy is split into three sections:

1. Data Management
2. Data Protection Act
3. Supporting Policies

This policy refers to the management of data, in all electronic, digital or physical formats. It also applies to any systems, processes, procedures and guidance for the management of data.

## Section 1 – Data Management

### 1.1 Aim

The Policy aim is to provide the standard to which data should be managed so that it protects the reputation of the organisation and enables value to be delivered to customers, stakeholders and investors.

In this Policy "data management" is used to describe the Company standard for collection, storage, retention, accessibility and reporting of data.

### 1.2 Context

Kelda Group values the importance of accurate and timely data for both decision making and business reporting. The importance of recording accurate and timely data helps safeguard the Company from misreporting and or incurring unnecessary cost.

As such the following principles have been established to provide a framework and standard for which the Company expects data to be managed.

### 1.3 Principles

Kelda Group commits to the following data management principles:

1. **Data is an asset** - Data is an asset that has value to the enterprise and is managed accordingly.

2. **Data is shared** – Colleagues should have access to the data that is necessary to perform their duties; therefore, data is shared across business functions.

3. **Data is collected with care.** – Data is collected and recorded in a manner that accurately reflects reality.

4. **The importance of data is understood** – Data that is required to report business performance is safeguarded and well managed to reflect this.

5. **Data is accurate & timely** - Data that is recorded is fit for purpose.

6. **Data is secure** - Data is protected from unauthorised use and disclosure.

Any risk associated with data shall be formally recognised in accordance to the Risk Management Policy.

Guidance on how to interpret these principles when handling data can be found in the Data Management operating manual referred to in Section 3.

## Section 2 - Data Protection Act 1998

The Data Protection Act 1998 applies to the Company's dealings and business affairs with customers, employees and certain third parties and seeks to ensure individuals are afforded adequate and proportionate levels of privacy.

The Company shall in its dealings with individuals comply with all relevant legislation in a manner which demonstrates the Company's regard for the privacy of individuals.

Information held relating to individuals and the way such information is processed is strictly regulated and the Company's intention is to promote full compliance by Group companies with both the spirit and the letter of the Act.

It is noted that the Company through its line managers has responsibility for the collection, storage and use of personal data. Employees also have responsibility under the Act and employees shall be instructed appropriately to ensure they do not disclose personal data other than in accordance with the Company's policy and procedures.

Employees shall also not use personal data for their own purposes and employees shall be made aware that the disclosure, or improper use of data may result in criminal prosecution and/or disciplinary action.

The Company recognises that a failure to comply with Data Protection legislation by the Company or its employees may result in criminal proceedings against the Company and any director, manager or company secretary (each of whom in certain circumstances can be held personally liable).

## Section 3 – Supporting Policies

This policy shall be read in conjunction with the other following policy and guidance documentation:

- Confidentiality Policy
- Risk Management Policy
- Data Management Operating Manual
- Information Security Policy & Guidance
- Document Retention Policy
- Data Classification Policy

**Version Control**
**Policy Owner:** Dave Mann, Governance and Compliance Manager
**Date of adoption:** 3 December 2015
**Date of last update/review:** 3 December 2015
**Date of next review:** December 2016