Title of Policy:	**Data Protection - Data Transfer Security**
Section:	**Human Resources**

Purpose

To inform and instruct all employees who handle personal data as to how it must be protected when transferred.

Statement

The Company stores a large volume of information electronically. This policy governs the procedures to protect this information and sets out how data should be transferred around the Company, and outside the Company, in a secure and protected way.

Procedure and Guidance

The law

Data storage is regulated by the General Data Protection Regulation. Standards are set out in the Regulation and the current Data Protection Act and one of the key points for consideration in a data transfer situation is that personal data must not be transferred to a country/territory outside the European Economic Area (EEA) unless that country/territory ensures appropriate safeguards.

Sensitive data

Sensitive data, for the purpose of this policy, includes data which contains:

- personal details about an individual (including those which are classed as special categories of data including data relating to health and race etc);
- confidential data about the Company;
- confidential data about goods, products or services;
- confidential data about Company, customers and suppliers.

If employees have any doubt as to whether data is or is not 'sensitive data', the employees must refer the matter to a member the Management Team.

Data transfers

Employees must seek consent from a member the Management Team to authorise the transfer of sensitive data. Data (sensitive or not) should only be transferred where it is strictly necessary for the effective running of the Company. Accordingly, before any data transfers are requested, the necessity of the transfer should be considered in advance. After authorisation has been granted, the data must be encrypted, compressed and password protected before it is sent.

Data transfers by post/courier

Data transfers which occur via physical media such as memory cards or CDs must only be dispatched via secure post. The use of first or second class Royal Mail is not permitted; only Special Delivery or Recorded Delivery should be used.

For non-Royal Mail services, a secure courier service must be used with a signature obtained upon delivery. The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack. The recipient should be advised in advance that the data is being sent so that they are aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The employee responsible for sending the data is responsible for confirming the data has arrived safely.

Lost or missing data

If an employee discovers that data has been lost or is missing, the employee is required to inform a member of the Management Team.

The Company's Breach Notification Policy will be followed. An investigation will be initiated immediately to establish the events leading to the data loss/theft and to determine whether a breach of personal data has occurred. If it has, a determination will be made as to whether the breach is notifiable under that policy.

A member of the Management Team must consider referring a matter to the police if it is found that unauthorised individuals have accessed sensitive data. Data which is held in the correct encrypted, compressed and/or password protected formats, which has been accessed by an unauthorised individual, has been accessed unlawfully.

Negligent data transfers

Employees who fail to comply with the requirements of this policy are likely to have their actions considered as gross misconduct, which may result in summary dismissal. Personal data breaches may result in exceptionally large fines for the Company.

Employees must not be negligent when transferring sensitive data. Examples of negligence include failing to obtain authorisation from a member the Management Team, failing to ensure the data is encrypted, compressed and password-protected, or using non-secure post services which are not tracked or insured.

KLOE References for this Policy	Regulations directly linked to this Policy	Regulation(s) relevant to this Policy
Safe **Well-Led**	**Regulation 9: Person-centred care** **Regulation 10: Dignity and respect** **Regulation 11: Need for consent**	