RED BIRD TUTORING

Data transfer security policy

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.

The law

Data storage is regulated by the General Data Protection Regulation (GDPR) and current domestic legislation. 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/tutors have any doubt as to whether data is or is not 'sensitive data', the employees must refer the matter to their manager.

Data transfers

Employees must seek consent from their manager 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 referred to the manager/ IT so that it can 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/tutor discovers that data has been lost or is missing, the employee/tutor is required to inform their manager who will also refer the matter to the Company's Data Protection Office.

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.

The manager 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/tutors 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 their manager, failing to ensure the data was not encrypted, compressed and password-protected, or using non-secure post services which are not tracked or insured.