OAKSWOOD COLLEGE

Data Protection & Security Policy

Registration Number: ZA182135

Data Protection Officer: Muhammad K Rehman

1. Introduction

The Oakswood College needs to collect personal information about people with whom it deals with, in order to carry out its business and provide its services. Such people include employees (present, past and prospective), customers (employers and learners), suppliers and other business contacts.

In addition, we may occasionally need to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. paper based or computer based system) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 1998.

The lawful and proper treatment of personal information held by the Oakswood College is extremely important to the success of our business and in order to maintain the confidence of our employees and customers, we commit to ensure that we treat personal information lawfully and correctly. The Oakswood College has a number of procedures in place to ensure privacy while protecting personal or corporate data and keep data protected from corruption and unauthorized access. The focus behind data security is based upon Encryption; Strong User Authentication and Reliable Backup Solutions.

2. The Principles of the Act

We support fully and comply with the eight principles of the Act, summarised below:

- Data shall be processed fairly and lawfully
- Data shall be obtained / processed for specific lawful purposes
- Data held must be adequate, relevant and not excessive
- Data must be accurate and kept up to date
- Data shall not be kept for longer than necessary
- Data shall be processed in accordance with rights of data subjects
- Data must be kept secure
- Data shall not be transferred outside the EEA unless there is adequate protection

3. Oakswood College - Commitment

The Oakswood College will:

- Ensure that there is always one person with overall responsibility for Data Protection
- Provide awareness for all staff members who handle personal information
- Provide clear lines of report and supervision for compliance with Data Protection
- Carry out regular checks to monitor and assess systems for processing of personal data

4 Oakswood College - Employee Commitment

Employees of the Oakswood College will, through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information
- Understand fully the purposes for which the Oakswood College uses personal information
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the company to meet its business needs or legal requirements
- Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required
- Not send information outside of the UK without the authority of their manager
- Ensure that the information is correctly input into the company's systems

5 Oakswood College – Learner commitment

When we collect any personal data, we will inform the individual why data is being collected and what it is intended to use it for.

Where we collect any sensitive data, we will take appropriate steps to ensure that we have explicit consent to hold, use and retain the information. Sensitive data is personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual orientation, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

We work and adhere to the Equality Act 2010 and some information which we need to look at with relation to passing information maybe except due to the safeguarding of Young Children and Venerable adults.

6 Requests for Personal Data

As defined within the Data Protection Act 1998, the Oakswood College will charge a fee of £10 for processing any request for personal data – this is known as a Subject Access Request.
Proof of identity is also required in the form of a driving licence, passport, recent utility bill etc.

Where a third party is making a request, a signed letter of consent from the data subject will be required. Some Subject Access requests may require further information before the process can commence. If this information is not received within 6 months of the request, the request will be closed and a new request will need to be made.

7 Security of Data

The Oakswood College are not currently certified to ISO 27001 Information Security Management Systems international standard. However we work with both privately funded and government funded schemes and have created information security processes and procedures to successfully meet the requirements of these contracts.

Information Security Policy

Introduction

The integrity and availability of information processed by the Oakswood College is paramount in order that the organisation may ensure the safety of its learners, clients and safety of its own personnel. It is important that all staff treat information security seriously in order that this purpose may be achieved.

Objective

The objective of this Policy is to protect information assets from all threats, whether internal or external, deliberate or accidental.

In support of this objective, the Director is committed to:

- Treating information security as a critical business issue
- Creating a security-positive environment
- Implementing controls that are proportionate to risk
- Achieving individual accountability for compliance with information security policies and supporting procedures.

Scope

The scope of this policy extends to:

- All information handled by the Oakswood College, its partners or its contractors processed electronically including printers and facsimile machines, such as:
    - Operational plans, accounting records, and minutes
    - Staff records
    - Learner records
- All processing facilities used in support of the Oakswood College's operational activities to store, process and transmit information, such as servers, PCs, printers and facsimile machines

Policy

As part of its over-arching business strategy and to meet its operational objectives, it is the policy of the Oakswood College to ensure that:

- Information and information processing assets will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Business requirements for the availability of information and information systems will be met
- Legislative and contractual obligations will be met
- Intellectual property rights and those of others will be protected and respected
- Business continuity plans will be produced, maintained and tested
- Unauthorised use of Oakswood College's information and systems will be prohibited, and the use of obscene, racist or otherwise offensive statements dealt with

- This Policy will be communicated to all staff and for whom information security training will be available
- All breaches of information security, actual or suspected, will be reported and investigated.

All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorized third party.

All personal data should be accessible only to those who need to use it and storage will consider both sensitivity and value of the information in question:

- In a lockable room with controlled access or
- In a locked drawer or filing cabinet or
- If computerized, password protected or
- Kept on other storage devices which are themselves kept securely

Care should be taken to ensure that PCs and terminals are not visible except to authorized staff and that computer passwords remain confidential. PC screens should not be left unattended without password protected screen savers and manual records should not be left where they can be accessed by unauthorized personnel.

Appropriate security measures must be in place for the deletion and disposal of personal data. Manual records will be shredded and hard drives of redundant PCs will be wiped clean before disposal.

This policy also applies to staff that process personal data away from the Oakswood College's premises. These staff must take particular care to ensure the safe and confidential storage of personal data and immediately report any potential risk or breach of company standards e.g. theft.

Review

This Policy will be monitored and formally updated annually.