SKERN ASSESSMENTS

Policy

Data Protection

Data Protection policy

EPA Data Protection Policy	
Applies to:	Employers, Training Providers, Apprentices, SA staff and Associated Third Parties
Effect from and replaces all previous versions prior to	10 August 2021
Owned By	Inspiring Learning
Reviewed and Monitored by	Head of IT
Document Location	Website & EPA resource area
Review Frequency	Annually

1. Purpose

The purpose of this policy is to set out the way in which data should be protected and handled within Kingswood.

2. Definitions

A large amount of data is stored electronically. It is essential that this data is carefully protected and transferred securely.

3. The law

The storing of all data must adhere to the standards set out in the Data Protection Act 1998. In particular it must be noted that personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of data protection.

The Data Protection Act 1998 is concerned with the processing of computerised and manual information about living individuals (personal data) and gives rights of access to the individuals who are the subject of that information. Further, the Act places certain obligations on the Company's data user, in respect of the personal information it processes or causes to be processed on its behalf by third parties.
This Act gives individuals the right to be aware of, seek access to and have some control over the nature and content of information held in relation to them by the Company, and to know for what reasons the information is held or processed. We recognise the importance of respecting the privacy of all our employees and therefore ensure that any information held will be dealt with properly and responsibly. The Act covers data that is processed automatically, held on computers and in manual files and applies to employees' personnel files, recruitment, health, attendance and disciplinary records and any other files compiled by management.

4. Company data

You must notify the HR Department of any change in your personal details or circumstances e.g. change of address or contact details, change in marital status or next of kin to contact in the event of being taken ill at work etc. so that your records are kept up to date and relevant.

In the course of employment, employees may have to handle personal and sensitive information that relates to individuals. If this applies to your work then the company requires that you observe the confidentiality of such information and ensure it is used, obtained or disclosed only in accordance with the company's right to do so, pursuant to its registration with the Information Commissioner.

Listed below are some of the main reasons the company holds personal information on employees:

- Recruitment & training
- Payroll
- Medical information related to sickness absenteeism
- Contacting next of kin in the event of an emergency
- Compliance with statutory requests from HM Revenue and Customs, Department of Work and Pensions, the Benefits Agency and other relevant public authorities/agencies
- Disciplinary purposes arising from an employee's conduct or ability to perform their job
- Provision of references to financial institutions and to assist potential future employers.

If you wish to know more about the personal details we hold concerning you, you should request this in writing and where we are obliged under the Data Protection Act 1998, we will give you the information you require upon payment by you of the appropriate statutory fee.

5. Transferring of data

Before any data is transferred the necessity of the transfer should be considered. Data should only be transferred when it is essential for the smooth operation of the company.

The transferring of any sensitive data must always be authorised by the Head of Department prior to it happening.

6. Definition of sensitive data

Any data which contains personal details about individuals is sensitive data. In addition, any data which contains confidential information about Kingswood, its products/services, its customers and its suppliers is sensitive data. If there is any doubt whether data would be classed as sensitive, the Head of Department should be consulted.

7. Data to be transferred

All sensitive or confidential data should be encrypted, compressed and password protected before transmission. If an employee does not know how to do this s/he should seek appropriate assistance from the IT department.

8. Memory sticks/CD-ROMs

If data is to be transferred through memory sticks, CD-ROMs or similar formats then the secure handling of these devices must be ensured. No such device should be sent through the open post – a secure courier service must always be used. The recipient should be clearly stated.

If data is sent via a courier the intended recipient must be made aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received, and liaising with the courier service if there is any delay in the receipt of the data.

9. Action to be taken if data goes missing

The Head of Department must be informed immediately if any confidential or sensitive data goes missing. An immediate investigation will be launched to discover where the data has gone.

If it is found that the data has been received by an unauthorised individual it must be determined whether that individual has accessed the data. If that individual has, and the data was correctly encrypted, compressed and password protected it suggests that the individual has unlawfully accessed the data. In such situations it might be appropriate to involve the police in the investigation.

The Head of Department will consider whether any individuals need to be informed about the data having gone missing – even if it is subsequently found. This might be necessary if there is a risk of personal data relating to individuals having been sent to the wrong person.

10. Negligent transfer of data

If an employee has been negligent in transferring sensitive and confidential data this might be considered to be gross misconduct, which might result in summary dismissal. This is particularly likely to be the decision if:

- The employee did not encrypt, compress and password protect data
- The employee transferred data using the open post and did not use a courier service
- The employee transferred data without seeking the appropriate approvals