Introduction

TES Training needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Company's data protection standards and to comply with the law.

This data protection policy will ensure TES Training:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers, suppliers and partners.
- Is open about how it stores and processes individuals' data
- Protects itself from the risk of a data breach.

Data Protection Law

The Data Protection Act 1998 (DPA) describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:-

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the EEA unless that country or territory also ensures an adequate level of protection.

The GDPR includes the following rights for individuals:-

1. The right to be informed;
2. The right of access;
3. The right to rectification
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. The right not to be subjected to automated decision-making including profiling.

Policy Scope

This policy applies to:-

- TES Training
- All staff of TES Training
- All contractors, suppliers and other people working on behalf of TES Training

It applies to all data that the Company holds relating to identifiable individuals, even if that information technically falls outside of the DPA 1998.

Responsibilities

Everyone who works for or with TES Training has some responsibility for ensuring data is collected, stored and handled appropriately.

Each Department that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, the Data Protection Officer is responsible for:-

- Keeping the Company updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data that TES Training holds about them (also called “subject access requests”)

General Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Employees should keep all data secure by taking sensible precautions and following the guidelines below.
- Strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Consent

On joining the Company, TES Training will seek your explicit signed consent for them to collect, retain and process your personal data. You have the right to withdraw your consent at any time, and this should be done either in writing to the HR Department or via e-mail to humanresources@tes2000.co.uk

Data Storage

These rules describe how and where data should be safely stored.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out:

- When not required, papers or files should be kept in a locked drawer or filing cabinet.
- Papers and printouts should not be left where unauthorised persons could see them e.g. printers.
- Data printouts should be disposed of securely when no longer required.

Where data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords and are never shared between employees.
- If data is stored on removable media these should be kept locked away securely when not in use.
- Data should only be stored on designated drivers and servers.
- Data should be backed up frequently.

- Data should never be saved directly to laptops or other mobile devices such as tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Accuracy

The law requires that the Company takes reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- TES Training will make it easy for data subjects to update the information the Company holds on them.
- Data should be updated as inaccuracies are discovered.

Subject Access Requests

All individuals who are the subject of personal data held by TES Training are entitled to:

- Ask what information the company holds on them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

If an individual contacts the Company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by completion of the Subject Access Request Form (Appendix 1) available from the HR Department.

The data controller will provide the relevant data within 28 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data For Other Reasons

In certain circumstances, the DPA allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, TES Training will disclose requested data. However, the data controller will ensure the request is legitimate before any data is released.

Data Breaches

TES Training's Data Protection Policy is intended to put in place processes and procedures to mitigate the risk of and data breaches. In the unlikely event of a breach this policy is to ensure that:

- Data breach events are detected, reported, categorised and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of disclosure
- Mitigation improvements are made and put in place to prevent recurrence
- Serious breaches can be reported to the Information Commissioner
- Lessons learnt are communicated to the organisation as appropriate and can work to prevent future incidents.

Incident Management

A Data Protection breach is the result of an event or series of events where Personally Identifiable Information (PII) is exposed to unauthorised or inappropriate processing that results in it security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the PII.

Breach management is concerned with detecting, reporting and containing incidents with the intention of implementing further controls to prevent the recurrence of the event.

TES Training will put measures in place to ensure that awareness of data protection will enable breaches to be reported more easily and issue guidance on how to report such breaches for analysis, categorisation and response. A log of incidents will be kept and periodic post reviews will be held to identify trends and continuous improvements to reduce the likelihood and impact of recurrence, as appropriate.

On discovery of a breach the following steps will be followed:

- Discovery
- Identify
- Assess
- Investigate
- Recommendations

These steps will be covered by use and completion of the Incident Management Form detailed in Appendix B.

Signature: 

Name: **Derek White**
Title: **Training Manager**
Date: **01 March 2019**
Review: **April 2020**

Section 1 – Applicant Details

Title (please tick one):	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Title (please state):
Forename(s):	
Family Name:	
Previous Family Name:	
Other name(s) known by:	
Date of Birth (dd/mm/yyyy):	……../……./……. Male ☐ or Female ☐

Current Address:	
Postcode	
Daytime Telephone No:	
Email Address:	
Previous Address:	
Postcode:	

Timescale

TES Training will endeavour to provide the information to you no later than 28 days after receiving the request, however if you have specific reasons for requiring data by a specific date please give details below:

(a) Date required:
(b) Reason (please state and supply supporting evidence):

Section 2 – Details of Information Required

Please use this space to give us any details about the information you are requesting, for example by stating specific documents you require (use extra sheets if necessary):

Section 3 – Declaration

The information which I have supplied in this application is correct, and I am the person to whom it relates or a representative acting on his/her behalf. I understand that TES 2000 may need to obtain further information from me/my representative in order to comply with this request.

Signature of Applicant:	Date:

Section 4 – Representative Details (if applicable)

Name of Representative:	
Company Name:	
Address & Postcode:	
Daytime Telephone No:	
Email Address:	

Section 5 – Proof of the Representative's identity

Please provide copies of two pieces of identification, one from list A and one from list B below and indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card

List A (photocopy of one from below)		**List B (plus one original from below)**	
Passport/Travel Document	☐	A letter sent to you by the Passport Office	☐
Photo driving licence	☐	Utility bill showing current home address	☐
Foreign National Identity Card	☐	Bank statement or Building Society Book	☐
	☐		☐
	☐		☐

Section 6 – Authority to release information to a Representative

A representative needs to obtain authority from the applicant before personal data can be released. The representative should obtain the applicant's signature below, or provide a separate note of authority.

This must be an original signature, not a photocopy (tip: using blue ink often helps verification).

If the applicant is signing as the guardian of a child under 12, proof of legal guardianship must also be provided.

I hereby give my authority for the representative named in Section 3 of this form to make a Subject Access Request on my behalf under the Data Protection Act 1998.	
Signature of Applicant:	Date:
Signature of Representative:	Date:

INCIDENT MANAGEMENT FORM

SUMMARY OF INCIDENT	
Date and Time of Incident	
Number of people whose data is affected	
Department	
Nature of breach e.g. theft/disclosed in error/technical problems	
Description of how breach occurred	
REPORTING	
When was breach reported?	
How you became aware of the breach:	
Date reported to Data Protection Officer	
PERSONAL DATA	
Full description of personal data involved (without identifiers);	
Number of individuals affected:	
Have all affected individuals been informed:	
If not, state why not:	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details:	
DATA RETRIEVAL	
What immediate remedial action was taken:	

Has the data been retrieved or deleted? If yes - date and time:	
IMPACT	
Describe the risk of harm to the individual as a result of this incident:	
Describe the risk of identity fraud as a result of this incident:	
Have you received a formal complaint from any individual affected by this breach? If so, provide details:	
MANAGEMENT	
Do you consider the employee(s) involved has breached information governances policies and procedures:	
Please inform of any disciplinary action taken in relation to the employee(s) involved:	
Had the employee(s) completed data protection training:	
As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been taken to address this:	
RCOMMENDATIONS	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure:	