November 2022

Training Strategies

Data Protection

Policy & Procedure

Policy Contents

The following policy has been approved by the Senior Leadership Team.

The policy will be reviewed on an annuals basis unless circumstances arise requiring the policy to be reviewed earlier.

Approved by Senior Leadership Team: November 2022

Planned review: November 2023

Applicability and Scope Statement:

This policy applies to all employees of Training Strategies regardless of role and location. Its provisions extend to those working on our behalf. Failure to adhere to this and associated policies, may lead to disciplinary proceedings up to and including dismissal.

This policy also applies to all of Training Strategies customers, sub-contractors, and partners.

NB: When working on external sites/establishments all staff need to make themselves familiar with any policies relevant to the specific working location

1.Aim

The policy and associated procedures aim to ensure that personal data is collected, stored, transferred and disclosed only in compliance with applicable legislation, primarily the Data Protection Act 1998 (DPA) and requirements of GDPR.

2.Scope

This policy applies to anyone collecting or processing personal data in connection with their work, studies or other activities in association with Training Strategies. The DPA and GDPR have broad applicability, covering all processing of personal data; it places additional restrictions and responsibilities on the processing of sensitive personal data.

See Appendix 2 - Key Principles for simple definitions of "data", "personal data" and "sensitive personal data".

3.Implementation

Training Strategies will ensure that:

1.A member of the Executive Team acts as the Strategic Data Protection Lead, supported by the Data Protection Officers in the business support department.

2.Meetings are held which introduce staff to the concept of a Data Protection Policy and to this policy; including staff induction, Management Team, and department team meetings; to enable ongoing dialogue around protecting personal data held by Training Strategies.

3.Support staff with primary responsibility for processing of personal and sensitive information receive training appropriate to their day to day duties and be required to maintain a level of operational understanding and awareness for the implementation of this policy and associated procedures. They will receive refresher training every 2 years.

4.All Training Strategies staff receive a level of training appropriate to their role, with refresher training every 3 years. This will be recorded and monitored through Workforce Development records.

5.Information technologies are used to ensure that this policy is accessible to all Training Strategies users.

4.Communication Flow

1.The policy is approved by the Training Strategies Directors.

2.The policy is communicated to all staff through staff induction, the staff intranet, email, training, and refresher training.

3.The Directors meet regularly to assure the implementation of the Data Protection Policy and requirements of GDPR, to keep up to date with legislation and guidelines and to identify issues arising.

4.Users of Training Strategies IT facilities and those with access to personal information receive a level of training appropriate to their role, with refresher training every 3 years. This is recorded and monitored through central Workforce Development records.

5.Monitoring of Implementation

The implementation of the Data Protection Policy is continuously monitored by the ICT Manager and assured by the Directors.

The Data Protection Policy is reviewed bi-annually by the Directors.

6.Associated Information and Guidance

The IT Acceptable Use Policy contains a fuller list of IT-related legislation; of relevance to the Data Protection Policy are:

- **Data Protection Act 1998**
- **Human rights Act 1998**
- **Data Protection (Processing of Sensitive Personal Data) order 2000**
- **GDPR**
- **Regulation of Investigatory Powers Act 2000**
- **Freedom of Information Act 2000**
- **Privacy and Electronic communications (EC Directive) Regulations 2003 (As amended)**

Further guidance:
The Information Commissioner's Office "Guide to data protection"
https://ico.org.uk/for-organisations/guide-to-data-protection/)
The Jisc "Data protection" guide (https://www.jisc.ac.uk/guides/data-protection)

7.Related Training Strategies Policies and Documents

The related documents below can be found on the staff intranet:

- Staff Code of Conduct
- Privacy Statement
- Learner Code of Conduct
- Information Security Policy
- IT Acceptable Use Policy
- Safeguarding Policy
- Disciplinary Policy

Appendices Documentation

A.1 - Privacy Notice
A.2 - Key Principles
A.3 - Responsibilities
A.4 - The Data Controller and Key Roles
A.5 - Subject Access Request Form
A.6 - Processing Sensitive Personal Data

A.1 – Privacy Notice
General

Training Strategies wants to protect the privacy of the staff, learners and stakeholders who give us their personal details. This privacy notice will help you understand how we use personal data. We may change our privacy policy at any time: changes will appear on the staff intranet, and you may wish to check the Privacy Notice each time you visit those sites. Whenever you give us personal data, you are consenting to its collection and use in accordance with this privacy policy.

What personal data do we collect?

We record information to enable our relationship with you e.g. we record staff bank details to enable salaries to be paid; we record checks of learner's financial circumstances to support bursary applications; we record contact details to enable us to correspond with you; we record monitoring information to enable us to monitor compliance with equality legislation. If at any time you are uncertain as to why a particular piece of information is required, please ask.

We monitor and record the use of Training Strategies IT facilities, as explained in the IT Acceptable Use Policy e.g. for the prevention, detection, and investigation of infringement of TSL regulations.

We log your Internet Protocol (IP) address when you visit a Training Strategies website. We use this to send and receive information to you over the Internet, as well as for analytics and performance monitoring.

How we use your personal data?

Depending on our relationship with you, we may use your personal data to provide goods and services to you or your organisation, to claim funding for your course, to determine and pay salaries. We may also use your personal data to support your education or development and in other routine ways e.g. recording attendance and achievement.

Whenever and wherever we collect, process, or use personal data, we take steps to ensure that it is treated securely and in accordance with our Data Protection Policy and UK law.

Staff contracts and learner's learning agreements give more details about the data collected, how it is used and to whom it may be disclosed. These are also where individuals expressly consent to this processing.

Refusal to consent, without good reason, to personal data being processed for these purposes may result in the withdrawal of an offer of employment or a place on a

course.

Any questions should be raised with our HR or Learner Records teams in the first instance and may be escalated to a Data Protection Offer (DPO) if required (see Appendix 4 - "The Data Controller and Key Roles").

To whom might we disclose your personal data?

The routine processing of your personal data may be carried out by TSL employees, agents, and data processors.

We may pass your personal data to third parties who need those data in order for us to provide you with requested services or to support your study at or work for TSL.

For example, if you are a learner we may pass your data to government agencies, to claim funding for your tuition; if you are a member of staff, we may pass your details to our bank, in order to pay your wages or to pension providers to process pension contributions.

We will ensure that your personal data continue to be protected, using contracts or other measures approved by UK data protection law.

Except as set out above, we will not disclose your personal data unless we are obliged to do so or allowed to do so by law. For instance, we are required to share certain staff data with HMRC.

Direct marketing

Unless you have already informed us that you do not wish us to do so, we may contact you by e-mail to market our goods and services. You may at any time request us to stop using your personal data for direct marketing purposes. If you wish to do this please contact: barrydunne@trainingstrategies.co.uk

Security

While no computer system or network can be guaranteed to be 100% secure, we will take appropriate steps to protect the security of your personal data.
Individuals have certain rights of access to their personal data. If you wish to request any information about your personal data, please see Appendix 5 - "Subject Access Request Form".

Retention

We keep different types of data for different, standard lengths of time, due to business need, funding and legal requirements. For details, see our "Records Management Policy".

Inaccuracies and Corrections

We would like to keep your personal data accurate and up to date. If you become aware of any errors or inaccuracies, please let us know by contacting:
barrydunne@trainingstrategies.co.uk
If you have any concerns about how we have handled your personal data, please contact:
barrydunne@trainingstrategies.co.uk
If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can complain to the **Information Commissioner's Office (ICO).**

A.2 - Key Principles

The Data Protection Act 1998 regulates the use of "personal data".

Key definitions of the DPA:

- **Data** is information held electronically but it could also include manual structured records.
- **Personal data** is any information which relates to, and identifies, a living person regardless of the format e.g. a learner's assessment, a training record for a member of staff, a learner's contact details.
- **Sensitive personal data** includes information about race, ethnic origin, political opinions, religious belief, trade union membership, physical or mental health, disability, sexual orientation and criminal record.
- **Processing** refers to any input, change, analysis, review, reporting, storage or output of data
- **Data controller** means a person who (either alone or jointly orin common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. (See Appendix 4 - "The Data Controller and Key Roles").
- **Data subject** means the individual whom particular personal data is about.

Note: In related TSL policies, personal data and information which is sensitive or confidential in some other way is grouped together as "Protected Information".

The Data Protection Principles

The DPA lists eight Data Protection Principles, which must be complied with. In summary, these state that personal data shall:

1.Be obtained and processed fairly and lawfully and only if specific conditions are met. (Additional conditions must be met in the case of sensitive personal data)
2.Be obtained specified and lawful purposes, and not processed in any manner incompatible with those purposes.
3.Be adequate, relevant and not excessive for those purposes.
4.Be accurate and kept up to date.
5.Not be kept for longer than is necessary for those purposes.
6.Be processed in accordance with the rights of data subjects under this Act.
7.Be protected by appropriate technical and organisational measures against unauthorised access and accidental loss, destruction or damage.
8.Not be transferred to a country outside the European Economic Area unless that country ensures an equivalent level of protection for personal data.

Conditions for Processing Personal Data

Personal data must not be processed unless specific conditions are met. Best practice (and the simplest to evidence compliance with) is for the data subject to have given their informed consent and for a record of that consent to be kept.

Processing may be permitted if an alternative DPA Schedule 2 condition is met. Guidance should always be sought from a Data Protection Officer (DPO) before processing personal data without informed consent.

NB: The police and similar agencies do not have an automatic right of access to individuals' personal data, they are required to provide specific, appropriately authorised requests. Any request from the police (or similar agency) should be referred immediately to a DPO - see Procedure 1 "Subject Access Request Procedure".

Conditions for Processing Sensitive Personal Data

There are additional restrictions on the processing of sensitive personal data. Best practice is for the data subject to have explicitly consented to the processing. Processing may be permitted if an alternative DPA Schedule 3 condition if met.

Guidance should always be sought from a Data Protection Officer (DPO) before processing sensitive personal data without explicit consent.

Additionally (due to the increased risk of harm if sensitive personal data were disclosed), Training Strategies places additional safeguards on the processing of this data. There is no general permission for staff to process this data; only explicitly authorised staff may process sensitive personal data.

The only situation in which an unauthorised member of staff may process sensitive personal data is when the processing is urgent and necessary. For example, an individual is unconscious and in need of medical attention and a member of staff tells the paramedic that the individual is pregnant.

See Appendix 6 for staff authorised to process sensitive personal data.

A.3 - Responsibilities

Responsibilities of staff

All staff are responsible for:

- Checking that any information they provide to Training Strategies in connection with their employment is accurate and up-to-date.
- Informing Training Strategies of any changes to information, which they have provided e.g. changes of address.
- Checking the information that Training Strategies will send out from time to time, giving details of information kept and processed about staff.
- Informing Training Strategies of any errors or changes. TSL cannot be held responsible for any errors unless the staff member has informed them.
- Complying with the guidance in this policy if and when, as part of their duties, they collect information about other people (e.g. about learner's coursework, opinions about ability, references toother academic institutions, or details of personal circumstances).

Ensuring that:

- Any personal data which they hold is kept securely (see below)
- Personal information is not disclosed orally or in writing, accidentally or otherwise to any unauthorised third party.
- Third-party requests should be handled via the Subject Access Request Procedure (Procedure 1)
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Responsibilities of learners:

Learners must ensure that all personal data provided to Training Strategies is accurate and up-to-date. They must ensure that changes of address etc are notified to Training Strategies Learners Records Department.
Learners who use Training Strategies computer facilities may, from time to time, process personal data. If they do, they must notify a Data Protection Officer (DPO) before beginning to process personal data and must comply with any guidance or direction from a DPO and with this policy. Any learner who requires further clarification about this should contact a DPO.

Securing Personal Data

Personal information should be:

Kept in a locked filing cabinet.
Kept in a locked drawer; or if it is computerised, be stored in a location on Training Strategies systems to which only those who need access to the data have access, and not on the internal disc drives of computers whether laptop or desktop, whether owned by TSL or not, except as permitted under the TSL Information Security Policy.
Kept solely on Training Strategies premises / systems and not removed, except as permitted under the Information Security Policy.

A.4 - The Data Controller and Key Roles

The Data Controller
Training Strategies Ltd as a body corporate is the data controller under the Act and is ultimately responsible for the implementation. However, the appointed Data Protection Officer will deal with day-to-day matters.

The Strategic Data Protection Lead and Senior Information Risk Owner
The Strategic Data Protection Lead and Senior Information Risk Owner functions reside within the Executive Team.

The Data Protection Officers
TSL has one Data Protection Officer, Samantha Lowe, who supports the Strategic Management Team and responsible persons on a particular aspects of data protection:

Contact details
The DPO can be contacted in person at 22 Oriel Road, Bootle, L20 7AD, by telephone at 0151-523-9655

A.5 - Subject Access Request Form

Overview
Training Strategies provides this "Subject Access Request Form" and guidance to assist data subjects in requesting information about personal data that we hold about them.

Process
To help us respond to your request, please complete the "Requester" sections, below.

Training Strategies will respond to your request within 40 days of whichever is the later of:

- Receipt of the Subject Access Request (SAR).
- Payment of the fee; any required clarification being obtained (e.g. Confirmation of identity or other information needed to find the personal data covered by the request).

The fee for processing of a SAR is £10.00. This should be paid via the Finance Office and the payment reference entered on the form below. The Finance Office can be contacted at the Oriel Road address or by telephone via the switchboard: 0151-523-9655. The fee may be waived in cases of economic hardship.

Requester - Confirmation of Identity:
We are required to confirm your identity before releasing personal data to you. To assist with this, please provide the information below. We may contact you to ask additional verification questions, to ensure that we only disclose personal data to the data subject.

Full name:
SAR fee payment reference:
Date of birth:
Learner's person code / Staff payroll no. (if applicable):
Contact number:
Contact email address:
Postal address:

Requester - Information Requested:
What information are you requesting?
(Please provide any details you can to help us locate the data you are requesting. For example, date range)

Third-Party Request:
If you are not the data subject, what is your relationship to the data subject and (if applicable) under what authority are you making the request (e.g. lasting power of attorney)

Please note: We have a duty to satisfy ourselves that any third party is entitled to act on behalf of the data subject (e.g. requiring proof of authority) and also to assess the data subject's capacity to understand and exercise their rights; for example there is a presumption that a child aged 12 years or more has the capacity to make a SAR. This may result in our declining a third-party request or responding to the data subject, rather than to the requester.

Form Submission and Any Questions:
Please send the completed form to: barrydunne@trainingstrategies.co.uk

A.6 - Processing Sensitive Personal Data

Training
Staff authorised to process sensitive personal data, will undergo additional training, to ensure they have the knowledge to appropriately safeguard this information, Including in applicable information security controls.

Staff authorised to process sensitive personal data.
Only explicitly authorised staff may process sensitive personal data.

Sensitive personal data will also be shared internally and with outside agencies to support learner's and staff welfare; for example, in requesting a "Safe and well" check from the Police. **Equality Impact Assessment Audit Proforma Audit Prompt**	**Response**
Name of policy:	Data Protection
Responsible Senior Manager:	Stephen Crewe
Who does the policy apply to: Staff Learners (please indicate which groups) Members of the general public (please specify who)	Staff, Learners, 3rd parties processing data on behalf of Training Strategies
Will the policy affect members of the target audience equally? If no, please indicate the specific groups targeted by the policy. In targeting the policy at a specific group of people will members of other groups be disadvantaged. If yes, how will this be addressed? What information has been gathered about the diversity of the target audience? Attach details of information considered. How has this diversity been considered in writing the policy?	Yes n/a n/a n/a

Does this policy contain visual images? If yes, are these technical or cultural in nature? If cultural, do they reflect diversity? If yes, please indicate how.	No n/a
Please indicate how this policy supports TSL in its General Equality Duty to:	Fair and transparent access to data by a subject allows them to scrutinise TSL in its dealings with the individual and provide evidence of how they have

Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act Advance equality of opportunity between people who share a protected characteristic and those who do not Foster good relations between people who share a protected characteristic and those who do not	been treated in the IAG, enrolment, study and progression and achievement of their courses.
Please indicate any negative impacts identified in relation to the protected characteristics listed below, or how you have arrived at the view that there are not negative impacts in relation to these characteristics: Age Disability Gender reassignment Marriage and civil partnership Race Religion or belief Sex Sexual orientation Pregnancy	n/a
Is the policy free from discrimination on the grounds of: Additional Learning Needs Economic Needs Social Needs	Yes Yes Yes
Please indicate who the policy has been considered by and/or who has been consulted about the policy. Where applicable include: Staff Health & Safety Committee Equality & Diversity Committee External groups (specify names) Advisory groups (specify names) Has the policy been posted on the staff/learner's intranet sites for consultation/review purposes? Did any equality issues arise from this?	

Can you identify any further consultations that might be necessary to ensure no adverse impact? If yes, please specify.	No
Can you identify any differential or adverse impact the policy might have that is not already recorded? If yes, please specify.	There is a small risk that learners who have physical or learning disabilities may not be able to access the provisions of the policy for subject access request and may therefore not be able to access the data held about them. As with all other forms of communication, TSL will provide advice, support and alternative methods where such issues are known to us.
Is this policy fit for purpose and in accordance with specific equality legislation? (Yes / No)	Yes

This policy is in conjunction with TSL's: Equality & Diversity Policy, Privacy Policy/Statement and Safeguarding Policy.