Training & Advisory Services Ltd.	**PERSONNEL POLICY**	
Reference: HR006	Version: 1.0	Number of Pages 2
TITLE:	**DATA PROTECTION**	
Authorised by: **Russell Prince** Chief Executive	Effective Date: Supersedes:	01/03/2016 14/05/2012

What is the impact of the data protection act 1998?

The Data Protection Act 1998 (DPA), states that anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure
- not transferred to countries without adequate protection.

This applies to SETA. Personal data includes both facts and opinions about the individual. SETA needs to understand the roles of those involved in processing and storing data about delegates and the need to understand the concepts of 'obtaining', 'holding' and 'disclosing' information. This information can be found on the Data Protection Act website.

Under the DPA, all delegates are entitled to request a copy of their educational records, free of charge, within 15 days of making a written request. If a candidate seeks access to his or her records, SETA should establish whether the delegate understands the nature of the request. If the SETA thinks the student/ work-learner does not understand owing to youth or immaturity, the request can be denied. If in doubt, we should seek guidance from the Office of the Information Commissioner.

Parents can request a copy of their child's educational record. The request should be made in writing, and SETA should supply the documentation within 15- days, free of charge or at no greater cost than that of supplying it. Where a delegate asks for a copy of his or her educational record, any charge must be no higher than the cost of supply or the cost allowed under the DPA, whichever is the lesser.

The DPA prevents disclosure of the following:

- material whose disclosure would be likely to cause serious harm to the physical or mental health or emotional condition of the pupil or someone else
- material concerning actual or suspected child abuse
- references supplied to potential employers of the pupil, any national body concerned with student admissions, another school, an institution of further or higher education, or any other place of education and training
- reports by a school to a juvenile court.

The DPA allows for this information to be transferred to another educational establishment. The DPA also allows, in some cases, for a record about a delegate from a third party, such as a letter from a parent, another delegate or a member of the local community, to be disclosed if it does not identify the third party. If it does identify the third party, it may still be disclosed if consent is given or if, in the circumstances, it is reasonable to allow disclosure without seeking that consent.

The most important changes of the new act include:

- what comprises a student/ delegate record
- what does not need to be disclosed
- the roles of those involved in entering, processing and storing personal data on candidates.

The seventh principle, relating to security, states that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". Guidance on what constitutes adequate security can be found in the legal guidance to the Data Protection Act 1998 available on the website.

SETA has a right and even a duty to monitor the use of the internet and email systems to prevent use for unlawful purposes or for distribution of offensive material. However, an individual has a right to privacy.

The first data protection principle states that data should be processed fairly and lawfully. Therefore, an organisation should be open on the subject of monitoring, and should also establish a code giving guidelines on the use of email and the internet and when individuals may use such systems for private communications.

With regard to email, SETA's stated policy is be to limit the use of email for private purposes. We then monitor the use of email to ensure that this is being adhered to. We also undertake spot checks rather than initiate a policy of continuous monitoring. In this way, SETA could monitor the use of email for private purposes but the actual content of the email messages could remain private. Again, however, any monitoring must be proportionate to the risk and designed to prevent rather than detect misuse.