POLICY ON THE USE OF PERSONAL DATA

The following is the ECTA policy on the use of **Personal Data** under the GDPR 2018 and Data Protection Act 1998

Policy on Use of Personal Data

The ECTA endorses fully the statements and the intent of the GDPR 2018 and Data Protection Act 1998 . The Data Protection principles contained in the Act are designed to protect the rights of the individual.

Definitions

Personal Data means data (manual or computer) which relate to a living individual who can be identified from those data (or from data and other information that is in the possession of, or is likely to come into the possession of, the data controller).

Data means information that is being processed automatically or is recorded with the intention that it should be processed automatically. Any manual data that forms part of an "accessible record" is also included in this definition.

Data Controller means a person who determines the way in which any personal data are to be processed.

Notification

Any time that data about an individual person is held manually or on a computer, the purposes must be: Available to be seen by the person named.

Processing

Every person must be sure that data held on manual and computer files about individuals is:

Processed fairly and lawfully	Kept private
Accurate and up-to-date	Kept only for as long as it is useful
Used only for defined purposes	Relevant and nor excessive

Disclosure

There should be a policy for confirming the identity of any person requesting information about themselves. This will be specific to the information system in question. For personal information requested by third parties the policy for disclosure will again be system and service specific. Formulating and implementing these policies will be the responsibility of the appointed person within the ECTA.

Any time that information from a file is given to a third party, the person giving the information must be sure that the third party is properly identified, and authorised and registered to receive the data Before disclosing personal information to a third party it is essential to check why the data is required and to whom that party intends to disclose it. ECTA will only disclose personal information when it has been checked that the disclosure is compatible with our disclosure policy and the Data Protection principles.

If you are aware of any data held or disclosures made that break the data protection principles you must report this to your supervisor or manager, in order that the breach may be addressed.
Policy on Authority to Access

The Computer Misuse Act 1990 identifies the legal framework for definition of and prosecution for unauthorised use or misuse of computers and computer systems. Whilst the Act is particularly intended to deal with unauthorised accesses from outside the organisation ("hackers"), it deals equally with unauthorised accesses from inside.

It is essential that you, as a computer user, understand the extent of your authority to use and access systems. Computers used for more than one purpose and those connected to a data network provide the potential for access to a large number of systems and to a great deal of personal, private and confidential data.

This policy makes it your responsibility to guard and protect your ability to access systems that you have authority to use. Passwords must not be written down or passed on (other than to your line manager). Computers must not be left logged in when unattended, particularly those in open access offices.

Any employee finding that they have access to systems and data which they are not authorised to use must report this to their supervisor or manager, in order that the access may be removed. Any employee with authority to access data that is no longer necessary to their work must ask for the access to be removed. Any employee who knows that unauthorised access is taking place must report this to their supervisor or manager, in order that the access may be removed.
Penalties under the Act fall into two main categories:

Unauthorised access - Anyone gaining access, or attempting to gain access to computer data they are not authorised to see, may face a fine of up to £2,000 or six months in prison, or both.
Ulterior intent or unauthorised modification - Anyone accessing data with an ulterior motive, or modifying data without authorisation, may be sentenced to up to five years in prison or an unlimited fine, or both.

Data Security Policy

- Make sure your password is changed regularly

- Do not leave your computer accessible when unattended (a password-protected screensaver can be a simple solution)
- Make sure you are authorised to use the systems you need
- Remember to copy data regularly for security and back-up.
- Ensure important email files are stored in an archive folder.

Contact us:

For more information, please contact:

ECTA
1st Floor Hadfield House
Gordon Street
Stockport
Cheshire
SK4 1RR
T: +44 (0)161 480 5656
hello@ectatraining.co.uk