

The TweDEX Group

Data Protection Policy

Introduction

The TweDEX Group is committed to protecting the rights and freedoms of data subjects, and securely processing their data in accordance with our legal obligations.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access during their work.

This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. <i>Business purposes include the following:</i> - <i>Compliance with our legal, regulatory and corporate governance obligations and good practice</i> - <i>Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests</i> - <i>Ensuring business policies are adhered to (such as policies covering email and internet use)</i> - <i>Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially</i>
--------------------------	--

	<i>sensitive information, security vetting, credit scoring and checking</i> - <i>Investigating complaints</i> - <i>Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments</i> - <i>Monitoring staff conduct, disciplinary matters</i> - <i>Marketing our business</i> - <i>Improving services</i>
--	---

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. <i>Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.</i>
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information –any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the

	processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is [the Information Commissioners Office].

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

Our Data Protection Officer (DPO), James Hair has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

Mr James Hair
Twedex Group,
214 Gyleview House
3 Redheughs Rigg
Edinburgh, EH12 9DQ

The Principles

The Twedex Group shall comply with the principles of data protection of the EU General Data Protection Regulation.

The Principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose

Data can only be collected for a specific purpose.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up to date.

5. Retention

We cannot store data longer than necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

Data Breaches

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Transworld Educational Experiences shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

[\(More information on the ICO website\)](#)