



IOEx Ltd

DATA PROTECTION & GDPR POLICY AND PROCEDURE

This document is approved and authorised for application within **IOEx Ltd**.

DOCUMENT CLASSIFICATION	Level 0 – Public
DOCUMENT REF	QAD 005
VERSION	0.1
DATED	27 th March 2024
DOCUMENT AUTHOR	AL
DOCUMENT REVIEW	27th March 2025

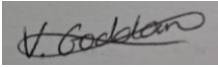
Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	27.03.24	AL	Creation of document as per organisation requirement

Distribution

NAME	TITLE
All team members	QAD 005 DATA PROTECTION & GDPR POLICY AND PROCEDURE

Approval

NAME	POSITION	SIGNATURE	DATE
Vicky Goddard	Director of the Academy		05/04/2024

This document is approved and authorised for application within **IOEx Ltd.**

Contents

IOEx Ltd Policy Statement	4
Policy scope	5
Responsibilities	5
Data storage	7
Data use	8
Data accuracy	8
Subject access requests	8
Disclosing data for other reasons	9
Providing information	9

This document is approved and authorised for application within **IOEx Ltd**.

DATA PROTECTION & GDPR POLICY & PROCEDURE

IOEx Ltd Policy Statement

IOEx Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees, learners, 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.

Why does this policy exist?

This data protection policy ensures IOEx Ltd:

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

Data protection law

The Data Protection Act 2018 describes how IOEx Ltd 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 any 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 European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

This document is approved and authorised for application within **IOEx Ltd**.

Policy scope

This policy applies to:

- ❖ The head office of IOEx Ltd

- ❖ All branches of IOEx Ltd

- ❖ All staff, learners, and volunteers of IOEx Ltd

- ❖ All contractors, suppliers and other people working on behalf of IOEx Ltd

It applies to all data that IOEx Ltd holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018 and GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals.

Data protection risks

This policy helps to protect IOEx Ltd from some very real data security risks, including:

- ❖ **Breaches of confidentiality.** For instance, information being given out inappropriately.

- ❖ **Failing to offer choice.** For instance, all individuals should be free to choose how IOEx Ltd uses data relating to them.

- ❖ **Reputational damage.** For instance, IOEx Ltd could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with IOEx Ltd has some responsibility for ensuring data is collected, stored, and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- ❖ The **Directors** are ultimately responsible for ensuring that IOEx Ltd meets its legal obligations.

- ❖ The **Quality Manager, Amanda Lewis** is responsible for:
 - Keeping the board updated about data protection responsibilities, risks, and issues.
 - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
 - Arranging data protection training and advice for the people covered by this policy.

This document is approved and authorised for application within **IOEx Ltd**.

- Handling data protection questions from staff and anyone else covered by this policy.
 - Dealing with requests from individuals to see the data IOEx Ltd holds about them (also called 'subject access requests').
- ❖ The **Financial Director and Interwork IT**, are responsible for:
 - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
 - Performing regular checks and scans to ensure security hardware and software is functioning properly.
 - Evaluating any third-party services IOEx Ltd is considering using to store or process data. For instance, cloud computing services.
 - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- ❖ The **Directors** are responsible for:
 - Approving any data protection statements attached to communications such as emails and letters.
 - Addressing any data protection queries from journalists or media
 - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff 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.
- ❖ **IOEx Ltd will provide training** to all employees to help them understand their responsibilities when handling data.
- ❖ Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- ❖ In particular, **strong passwords must be used**, and they should never be shared.
- ❖ Personal data **should not be disclosed** to unauthorised people, either within IOEx Ltd 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 Quality Manager if they are unsure about any aspect of data protection.

This document is approved and authorised for application within **IOEx Ltd**.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Quality Manager or the Finance Director.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

- ❖ When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- ❖ Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- ❖ Data printouts should be shredded and disposed of securely when no longer required.

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

- ❖ Data should be protected by strong passwords that are changed regularly and never shared between employees.
- ❖ If data is stored on removable media, these should be kept locked away securely when not being used.
- ❖ Data should only be stored on designated drives and servers and should only be uploaded when approved.
- ❖ Servers containing personal data should be sited in a secure location, away from general office space.
- ❖ Data should be backed up frequently. Those backups should be tested regularly, in line with IOEx Ltd and Interwork IT backup procedures.
- ❖ Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- ❖ All servers and computers containing data should be protected by approved security software and a firewall.

This document is approved and authorised for application within **IOEx Ltd**.

Data use

Personal data is of no value to IOEx Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- ❖ When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- ❖ Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- ❖ Data must be encrypted before being transferred electronically.
- ❖ Personal data should never be transferred outside of the European Economic Area.
- ❖ Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires IOEx Ltd to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort IOEx Ltd should put into ensuring its accuracy. 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. For instance, by confirming learner's details when they are in direct contact.
- ❖ Data should be updated as inaccuracies are discovered. For instance, if a learner can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by IOEx Ltd are entitled to:

- ❖ Ask what information IOEx Ltd holds about them and why.
- ❖ Ask how to gain access to it.
- ❖ Be informed how to keep it up to date.
- ❖ Be informed how IOEx Ltd is meeting its data protection obligations.

This document is approved and authorised for application within **IOEx Ltd**.

If an individual contacts IOEx Ltd requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Quality Manager at amdanda.lewis@export.org.uk

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The Quality Manager 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 Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, IOEx Ltd will disclose requested data. However, the Quality Manager will ensure the request is legitimate, seeking assistance from the Directors and from the company's legal advisers where necessary.

Providing information

IOEx Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- ❖ How the data is being used
- ❖ How to exercise their rights

This document is approved and authorised for application within **IOEx Ltd**.