

Data Protection Policy

General Data Protection Regulations 2021

**Data protection policy**

# Key details

* Policy became operational on: 1st March 2018
* Next review date: 31st January 2026

# Introduction

As part of our business, we at ioda Ltd need to gather and use certain information about individuals including our:

* Customers
* Learners
* Apprentices
* Suppliers
* Business contacts and partners
* Employees 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 this policy exists

This data protection policy ensures ioda Ltd:

* Complies with data protection law and follows good practice
* Protects the rights of staff, customers and partners and anyone we deal with
* Is open and transparent about how it stores and processes individuals’ data
* Protects itself from the risks of a data breach

# Data protection law

The General Data Protection Regulation 2018 (GDPR) described what and how organisations, including ioda Ltd, must collect, handle and store personal information, including its disposal and when it must be deleted. Since exiting the EU and the end of the transition period, as the EU GDPR is an EU Regulation, it no longer applies to the UK. However, as ioda operate inside the UK, we have to comply with UK data protection law.

The GDPR has been incorporated into UK data protection law as the UK GDPR and therefore, there is little change to the core data protection principles, rights and obligations found in the UK GDPR. The GDPR narrations continue to have the same status as before.

The Data Protection Act 2018 (DPA 2018) continues to apply. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information collected must be used fairly, stored safely, not disclosed unlawfully and deleted within stipulated timescales.

The GDPR 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

Transfers of data from the UK to the European Economic Area (EEA) was not restricted following Brexit. The EU agreed to delay transfer restrictions from the EEA to the UK until 30 June 2021 (known as the bridge). This enabled personal data to flow freely from the EEA to the UK until either adequacy decisions are adopted, or the bridge ends.

On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority of circumstances.

These decisions are expected to last until 27 June 2025.

# People, risks and responsibilities – Scope of policy

This policy applies to:

* The head office of ioda Ltd
* All locations where ioda Ltd staff work including home office accommodation
* All staff and associates of ioda Ltd
* All contractors, suppliers and other people working on behalf of ioda Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR UK legislation, it will be treated as coming under them. This list of data that is collected is listed in the privacy policy and in the register of processing activities as collected and reviewed every year in compliance with the ICO guidance.

# Responsibilities

Everyone who works for or with ioda Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each individual or team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

* The **board** is ultimately responsible for ensuring that ioda Ltd meets its legal obligations and there is an appointment designated data protection officer (DPO) and risk review board at group level.
* The Data Protection Officers are responsible for:
  + Keeping themselves and staff 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.
  + Handling data protection questions from staff and anyone else covered by this policy.
  + Dealing with requests from individuals to see the data ioda Ltd holds about them (also called ‘subject access requests’).
  + Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data. Including conducting any DPIA’s as required
  + Ensuring data is deleted within agreed and appropriate timescales.
  + Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  + Evaluating any third-party services, the company is considering using to store or process data and ensuring, as partners, they perform regular checks and scans to ensure security hardware and software is functioning properly, for instance, cloud computing services.
  + Approving any data protection statements attached to communications such as emails and letters.
  + Addressing any data protection queries from journalists or media outlets like newspapers.
  + Where necessary, working with staff to ensure marketing initiatives abide by data protection principles

**Data breach**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

**Data breach process**

If a personal data breach is experienced by any ioda employee, this must be reported to the designated data protection officers or head of training within 24 hours. The process will consider whether this poses a risk to the individual(s) concerned and further consider the likelihood and severity of the risk to people’s rights and freedoms, following the breach.

When this assessment has been made, if it’s likely there will be a risk then the DPO must be notified and subsequently a judgement of if to notify the ICO; if it’s unlikely then the DPO does not have to report it to the ICO. Every breach does not have to be reported to the ICO.

Where a breach is informed to the ICO, this breach is also informed immediately to the client representative and data subject.

The breach of information regardless of risk and impact should be recorded on a Data Breach form and saved on the shared drive.

**General guidelines for staff**

* 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.
* iodaLtd **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. Only the person whose password it is should be aware of the passwords.
* Personal data **should not be disclosed** to unauthorised people, either within the company 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.
* Data **must always be stored and erased** as outlined in this policy.
* Employees **should request help** from their line manager or Data Compliance Officer (DCO) if they are unsure about any aspect of data protection.

**Data storage rules**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to their line manager or company DCO.

**Hard copies**

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

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

* When **unoccupied**, **the main office** must always remain locked and secure with the alarm system activated.
* When not required and working from home, any 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**, e.g. on a printer, or in classrooms where delegates are present.
* **Data printouts should be shredded** and disposed of securely when no longer required.

**Electronic data**

* 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.
* When leaving a workstation, screens should be locked and never left unattended with data showing or access to personal accounts being available.
* Data should never be **stored on removable media** (like a USB stick, CD or DVD)
* Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing services**.
* 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 the company’s standard backup procedures.
* All company laptops must be kept in a secure place when not in use. They must not be left in vehicles overnight and if travelling during the day and the vehicle is unattended must be stored out of sight in the boot.
* All company laptops must be encrypted through password access and data saved directly to this device erased in line with the erasure rules detailed in this policy
* All laptop data must be saved directly onto the companies secure shared cloud facility.
* Data should **never be saved directly** to mobile devices such tablets or smart phones.
* All servers and computers containing data should be protected by **approved security software and a firewall**.
* Data will be stored for the following periods:
  + Employee Details: During terms of employment and a period of six (6) years after contract termination or their 75th birthday, whichever is sooner
  + General Client Data: Five years for all clients other than research related
  + Learner Details: For those attending:
    - Accredited programmes – Six years (from completion date)
    - Apprenticeship programmes – Six years (from completion date)
    - Non-accredited – Three years (from completion date)
  + Supplier Details: Five Years after termination of business relationship.
  + Business Partner Details: Five Years after termination of business relationship.
  + Finance Data: Seven Years

**Electronic data stored by our suppliers**

Where personal data is stored by our suppliers, they must store this within the EEA to meet the requirements of our clients.

Sometimes, a third country may be declared as offering an adequate level of protection through a European Commission decision (‘Adequacy Decision’), meaning that data can be transferred with another company in that third country without the data exporter being required to provide further safeguards or being subject to additional conditions. In other words, the transfers to an ‘adequate’ third country will be comparable to a transmission of data within the EU. In the absence of an Adequacy Decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals. Such appropriate safeguards include:

* In the case of a group of undertakings, or groups of companies engaged in a joint economic activity, companies can transfer personal data based on so-called binding corporate rules.
* Contractual arrangements with the recipient of the personal data, using, for example, the standard contractual clauses approved by the European Commission.
* Adherence to a code of conduct or certification mechanism together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data.
* Finally, if a transfer of personal data is envisaged to a third country that isn’t the subject of an Adequacy Decision and if appropriate safeguards are absent, a transfer can be made based on a number of derogations for specific situations for example, where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer.
* All data storage information by suppliers, or anyone contracted to provide a service are requested at project set up and saved internally for reference including their implemented safety measures.

**Data destruction**

Data destruction takes place on a rolling basis – as dictated to by the retention schedule each type of data is subject to and the date it passes these retention period

Paper copies will be shredded and a certificate of proof obtained from a third party or shredded in-house with Manager oversight.

Electronic data held on all devices will be securely destroyed (e.g. overwritten, reformatted, firmware-based erasure, physical data media destruction).

**Data erasure and off boarding rules**

All persons whose details are held by ioda have the right to request erasure and the right to be forgotten from data subjects. Client off boarding is defined as the proactive management and removal of redundant, obsolete or incorrect information and data held by ioda.

In order to meet these requests in an adequate and timely fashion ioda will apply the following procedure.

1. **Assess request**

Once the request is received from a data subject, ioda will assess the request and determine if it has legal basis to hold onto the data. If not, then ioda must strive to identify all the repositories and systems that contain this personal information on the data subject.

1. **Determine the impact of off boarding on the data subject**

If it is decided to off board the data, then it is important to check for any interdependencies on the data that may impact on other data subjects. Once a full understanding of the data subject’s associations and activities is gained, the process to disassociate reliant parties can commence.

1. **Off boarding the data**

To ensure full auditability of the process, ioda will add in a reason why off boarding is taking place (e.g. request for erasure by data subject). A DCO should approve the off-boarding process before being marked as complete.

1. **De-activating from IT systems**

The final step in the off-boarding process involves ensuring that the information cannot be further used by ioda. This should include a notification that the data has been successfully off boarded or quarantined from all related IT systems.

1. **Confirm erasure of data**

The final step involves a confirmation in writing to the data subject that the data has been effectively erased or quarantined from all internal systems in compliance with their request under GDPR.

1. **Offboarding breach response**

Staff must report a breach of this off boarding rule to a DCO without undue delay and where feasible no later than 72 hours once a breach has been identified, except where the personal data breach is unlikely to result in a risk to the rights and freedoms of a data subject.

**Data use**

* 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**. Guidance will be provided if required.
* Personal data should **never be transferred outside of the European Economic Area** unless an approved reason is established (see above).
* Employees should try not save copies of personal data to their own computers by accessing and updating the central copy of any data.
* However, if personal data is saved, then the outlined security and deletion protocols must be observed.
* When using any AI programme to process data - ensure that no bias related risks or loss of integrity are inherent in the use of any such technology. This includes **Never putting any explicit personal information into chat bots or software such as Chat GPT or Co-Pilot**

**Data accuracy**

The law requires ioda 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 we at ioda will 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 a customer’s details when they call.
* ioda Ltd will make it **easy for data subjects to update the information** we hold about them. For instance, via the company website.
* Data should be **updated as inaccuracies are discovered**. For instance, if a customer 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 ioda Ltd are entitled to:

* Ask **what information** the company holds about them and why.
* Ask **how to gain access** to it.
* Be informed **how to keep it up to date.**
* Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a ‘subject access request’.

Subject access requests from individuals should made by email, addressed to [info@ioda.com](mailto:info@ioda.com) This can also be requested verbally and by informal means and training to staff will be provided on how to identify a subject access request.

Individuals can make an initial request for information free, and subsequent requests, or requests that are deemed manifestly unfounded or excessive will be charged £10 administration fee per subject access request. The organisation will aim to provide the relevant data within 14 days.

The DCO will always verify the identity of anyone making a subject access request before handing over any information and will never share any data with external third parties without consent. We will also never use any personal data for direct marketing unless explicitly agreed with data subjects and the option to opt in is provided.

**Disclosing data for other reasons**

In certain circumstances, the GDPR UK allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ioda Ltd may disclose requested data. However, the organisation will ensure the request is legitimate, seeking guidance from the company’s legal advisers where necessary.

**Providing information**

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

* How the data is being used
* How to exercise their rights

To these ends, the company has a privacy statement, (See appendix one) setting out how data relating to individuals is used by the company and is available on request

Our Policy is reviewed annually by our Information & Data Manager, following our Quality Calendar and is authorised by our Chief Executive.



Approved by: Lisa Reynolds

Last review date: December 2024

Next review date: January 2026

**Change log**

| Date & version | Changes made |
| --- | --- |
| 26/01/2022  V2022 | * Addition of change log * Addition of last review date * Removal of Director titles * Addition of review process and timing * Change to information relating to post-Brexit data bridge & addition of next GDPR EU review date * Removal of reference to marketing database information removal linked to industry suppression files * Removal of reference to a standard form as we do not provide one |
| 07/06/22  V2022 | * Addition of data retention period for apprenticeships as six years (as per the ESFA guidelines) |
| 02/09/22  V3 | * Update Privacy Notice- Appendix 1- updated to reflect data processing changes via LMS |
| 23/08/2023  V2023 V1 | * Update of retention information for employees following termination of employment. * Addition of finance retention policy guidelines * Page 7 – update to apprenticeship retention from completion date to Financial Year End after the end of the course |
| V2024 | * No amendments |
| 11/09/24  V2024 | * Definition of paper and electronic data * Inclusion of data storage outside of the EEA * Removal of Sally Dale and Sean Stokoe and replacement with Lisa Reynolds |
| 16/10/24 | * Addition of advising to clients of data breach |
| 10/12/24 V2 2025 | * Update to info relating to the transfer of data outside EEA * Include Direct Marketing * Removal of Sally and Sean as Directors * Include reference to Group level responsibilities and more detail on risk management * Include yearly ROPA and asset reviews * Update to retention schedule details * Add certification to privacy statement purposes * Add unintentional bias and loss of integrity in AI use |

# Appendix One

ioda **Ltd - Privacy Notice**

This privacy policy explains how ioda Limited of 4 Grimston Grange Offices, Grimston Park, Tadcaster, LS24 9BX, company number 3352708 (‘ioda Ltd’, ‘We’, ‘Us’), uses information about current and prospective customers, employees and apprentices.

**The type of personal information we collect:**

We currently collect and process the following information:

* Learner information that can include:

Name

Any previous names

Postal Address

Contact details such as email address and telephone number

National Insurance Number

Date of Birth

Equality Monitoring Data

Place of work

Proof of ID

Next of Kin

Job Title and place of work

Learner specific identifying data such as ULN and qualification registry numbers

Opinions and service feedback

Financial information such as contracts and payments

Learner Progress

Qualification details and prior attainment/learning

Details of personal circumstances that may result in an impact on learning

* Client information that can include:

Name

Contact information such as email and telephone number

Job title

Opinions and service feedback

Financial arrangements

* Employee information that can include:

Name

Next of Kin

Address

National Insurance number

Telephone

Email

Employment history

Training records

Bank details

Confirmation of ID

**How we get the personal information and why we have it**

The personal information we control, and process is provided to us directly by you for one of the following reasons:

* Apprenticeship registration
* Qualification registration
* Qualification certification
* Survey completion
* Learner Management System registration
* Completion of work
* Employment

We also receive personal information indirectly, from the following sources in the following scenarios:

* Workplace communications relating to an individual’s learning
* Coach/Mentor/Trainer communications relating to learning
* Qualification awarding bodies, where copies of certificates are requested
* Qualification/Awarding bodies reporting functions
* LMS reporting functions
* Website Cookies

We use the information that you have given us to:

* Provide an Apprenticeship Learning Provider service
* Provide training and qualifications
* Support your individual needs and progression
* Comply with HSE, ESFA, DfE, Ofsted, financial regulations, employment law and the Equality Act 2010
* Communicate with you and where necessary your employer
* Quality assure and improve our service
* Provide Payroll and other employment services

With exception to the above we never share your information with any third parties and will never directly use your contact details for marketing purposes without explicit consent.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing this information are:

**(a) We have a contractual obligation.**

**(b) We have a legal obligation.**

**(c) We have a legitimate interest.**

**(d) We have been provided consent.**

**How we store your personal information**

Your information is securely stored in our Learner Management System. We also securely store information in our organisational SharePoint. Details of ioda Data security and protection policy can be requested by contacting the business support team at the address below.

We are required by the Education and Skills Funding Agency to retain your information for six years for auditing and funding purposes. This is the maximum amount of time we will store any data. This is stored securely and fully deleted from our systems once this time has passed.

Any other information will be fully deleted once the original lawful basis for collecting and storing has passed. This is reviewed on a regular basis along with our scheduled data retention audits and update of the register of processing activities.

**Your data protection rights**

Under data protection law, you have rights including:

**Your right of access** - You have the right to ask us for copies of your personal information.

**Your right to rectification** - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

**Your right to erasure** - You have the right to ask us to erase your personal information in certain circumstances.

**Your right to restriction of processing** - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

**Your right to object to processing** - You have the the right to object to the processing of your personal information in certain circumstances.

**Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

**Changes to our privacy policy**

We keep our privacy policy under regular review, and we will place any updates on this web page. This privacy policy was last updated in December 2024

# How to contact us

Please contact us if you have any questions about our privacy policy or information, we hold about you via the following:

Email: info@ioda.com

Telephone: 01937 831414

By post: ioda Ltd

Data Privacy

4 Grimston Grange Offices, Grimston Park

Tadcaster

LS24 9BX