Data Protection Policy

UK GDPR

Document Control	
Title	Data Protection Policy - GDPR
Date of review	03/12/2025 (Legislation update)
Document Owner	Salih Yilmaz & Zelin Mumtaz

Version Control History

Date	Paragraph/section amended	Reason	New issue no.
28/12/2022	Created		V1
28/11/2023		Annual Review	V2
01/05/2024		Annual Review	V3
13/06/2025		Annual Review	V4
03/12/2025	**V5 (Dec 2025):** Full rewrite to align with UK GDPR and Data Protection Act 2018 (as amended), including DUAA 2025 changes (complaints handling, SAR search standard and "stop the clock" readiness, cookies/storage and access technology exceptions, transfer test updates).	Legislation update	V5
05/05/2026		Annual Review	V6

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

Contents

1. Status and supporting documents

This policy is supported by (and should be read alongside) Intech Centre's operational procedures and logs, including:

- Subject Access Request (SAR) and rights request procedure
- Data protection complaints procedure
- Personal data breach / incident procedure
- Retention schedule and destruction log
- Supplier/processor register and due diligence checklist
- DPIA (Data Protection Impact Assessment) template and register
- Privacy notices (Learners 19+, Staff/Applicants, Website/Cookies)

2. Purpose and policy statement

Intech Centre is committed to protecting the rights and privacy of individuals and to handling personal information lawfully, fairly and transparently.

We recognise that we must demonstrate **accountability** in how we use personal data. This includes having clear policies, staff training, secure systems, appropriate retention and disposal controls, and documented decision-making about data sharing and privacy risks.

This policy explains how Intech Centre will collect, use, store, share and dispose of personal data in compliance with:

- the **UK General Data Protection Regulation (UK GDPR)**;
- the **Data Protection Act 2018**, as amended; and
- the **Privacy and Electronic Communications Regulations (PECR)** (where applicable), including changes introduced by the **Data (Use and Access) Act 2025 (DUAA)**.

3. About Intech Centre and what we do

Intech Centre is an education centre supporting **adult learners aged 19 or over**. We provide:

- careers information, advice and guidance;
- training and learning programmes; and
- examinations and related administration

To deliver these services properly and safely, we must process certain personal information about learners, staff, and other individuals with whom we have a relationship.

4. Scope and who this policy applies to

This policy applies to:

- all Intech Centre staff (permanent, temporary, casual);
- contractors, consultants, volunteers and agency staff working on our behalf;
- learners and prospective learners (19+);
- visitors (including CCTV where used); and
- third-party suppliers who process personal data for us (processors).

This policy covers personal data in all formats, including:

- paper/manual files;
- electronic records (systems, shared drives, emails);
- photographs and video (including marketing where used);
- CCTV footage (where used); and
- cloud-hosted services.

4.1 Compliance and disciplinary expectations

All staff and contractors must comply with this policy. Any breach may be treated as a disciplinary matter (or contractual breach for contractors) and may require reporting to the ICO and/or affected individuals where legally required.

5. Definitions

Personal data means information relating to an identified or identifiable living person (e.g., name, contact details, learner number, exam records, CCTV images).

Special category data includes health/disability information (e.g., for reasonable adjustments), racial/ethnic origin, religious beliefs and other sensitive categories.

Criminal offence data is personal data relating to criminal convictions/offences or related security measures.

Processing includes collecting, recording, storing, using, sharing, and deleting personal data.

Controller determines why/how data is processed. **Processor** processes data on the controller's behalf.

6. Data protection principles

Intech Centre will comply with the UK GDPR principles. Personal data must be:

1. **Processed lawfully, fairly and transparently**
2. **Collected for specified, explicit and legitimate purposes** and not used incompatibly
3. **Adequate, relevant and limited** to what is necessary (data minimisation)
4. **Accurate and kept up to date** where necessary
5. **Kept no longer than necessary** (storage limitation)
6. **Processed securely** (integrity and confidentiality)
7. **Handled with accountability**, meaning we can demonstrate compliance

We apply these principles in practice through privacy notices, lawful basis assessment, access controls, retention schedules, staff training, DPIAs, supplier management, and logging of key actions (SARs, complaints, breaches, destruction).

7. Governance, roles and responsibilities

7.1 Data controller

Intech Centre is the **data controller** for the personal data it processes for its own purposes. This means we determine why and how personal data is processed.

7.2 Data Protection Lead / DPO contact

Intech Centre appoints a Data Protection Lead (DPO contact), currently: **Salih Yilmaz, Senior Manager**

The Data Protection Lead is responsible for:

- advising on data protection obligations and good practice;
- ensuring privacy notices and consent statements are appropriate and up to date;
- coordinating and responding to SARs and other rights requests;
- operating the data protection complaints process (including DUAA requirements);
- overseeing incident/breach management and decisions on notification;
- maintaining key compliance records (logs/registers);
- ensuring staff training and awareness is delivered and recorded; and
- overseeing supplier/processor compliance and contract controls.

7.3 Responsibilities of all staff and contractors

All staff and contractors must:

- treat personal data as confidential and handle it only for legitimate work purposes;
- use approved systems and follow security requirements;
- check recipient details before sending personal data by email or other means;
- store paper files securely and return them to secure storage when not in use;
- report any data breach, suspected breach, SAR, or complaint immediately to the Data Protection Lead; and
- complete required training and follow operational procedures.

8. What personal data we process (Intech Centre context)

8.1 Learners and prospective learners (19+)

We may process:

- identity and contact details (name, address, date of birth, phone, email);
- enrolment information and eligibility evidence (where needed);
- course/learning information (attendance, progress, assessments, achievements);
- careers advice and guidance information (appointment notes, action plans where used);
- examination information (candidate registration, entries, results, certification);
- reasonable adjustments and access arrangements information;
- fees and finance information (invoices, payments) where applicable;
- safeguarding and welfare information (where necessary and lawful);
- communications (email, phone notes) relating to services we provide; and
- CCTV images (where CCTV is in operation).

8.2 Staff, applicants and contractors

We may process:

- recruitment and employment information (applications, CVs, references);

- right-to-work evidence and identity checks;
- payroll and finance information (where applicable);
- training records, performance/disciplinary information (where necessary);
- absence and health information (where necessary, with safeguards);
- IT security and access logs (for security and continuity).

8.3 Website users (where applicable)

We may process:

- enquiry form details and communications;
- technical information (IP address, browser/device data);
- cookies and similar technologies (see Section 19).

9. Why we process data and lawful bases

We identify a lawful basis under Article 6 UK GDPR for each processing activity.

9.1 Typical purposes (tailored to Intech Centre)

We process personal data to:

- deliver careers advice, training and examinations;
- register learners with awarding bodies and manage exam entries/results/certification;
- provide learner support and reasonable adjustments;
- monitor attendance, progress and achievement;
- manage fees, invoices and payments where applicable;
- recruit, manage, pay and train staff and contractors;
- maintain safeguarding and welfare arrangements where necessary;
- keep our premises, staff and learners safe (including CCTV and visitor management where used);
- operate our IT systems and protect against security threats; and
- comply with legal, regulatory, contractual, audit or funding requirements.

9.2 Lawful bases we rely on

Depending on the activity, we rely on one or more of:

- **Contract** (e.g., delivering training, providing agreed services, administering examinations);
- **Legal obligation** (e.g., employment/tax obligations, certain reporting duties);
- **Legitimate interests** (e.g., running the centre, security, fraud prevention, safeguarding and welfare management, internal administration—balanced against individual rights where required);
- **Consent** (e.g., marketing photos/testimonials; some marketing communications where required);
- **Vital interests** (rare; emergency situations); and
- **Public task** (only where clearly applicable to a specific activity/arrangement).

9.3 Recognised Legitimate Interests (DUAA)

The DUAA introduces **recognised legitimate interests**, which can apply to certain specified purposes (e.g., safeguarding, emergencies, and crime prevention). Where applicable, Intech Centre will rely on this only when lawful and necessary, and we will document the purpose and safeguards used.

10. Special category data and criminal offence data

10.1 Special category data

We only process special category data where:

- it is necessary for a defined purpose; and
- we have:
    - an Article 6 lawful basis; and
    - an Article 9 condition (and, where required, a DPA 2018 Schedule 1 condition).

In an adult education and exams context, this most commonly includes health/disability information to:

- arrange **reasonable adjustments** and learning support; and/or
- manage welfare and safeguarding where necessary.

Safeguards include:

- collecting only what is required (minimisation);
- restricting access to authorised staff on a need-to-know basis;
- secure storage (restricted folders/locked cabinets);
- clear retention and secure destruction rules; and
- heightened care when sharing externally (e.g., awarding bodies for adjustments).

10.2 Criminal offence data

We will only process criminal offence data where lawful, necessary and proportionate, with restricted access and controlled retention.

11. Transparency and privacy notices

We provide privacy information that is clear and accessible, explaining:

- what we collect and why;
- lawful bases;
- who we share with;
- retention;
- rights and how to exercise them; and
- how to complain.

We maintain (and publish/issue where appropriate) separate privacy notices for:

- learners (19+);
- staff/applicants; and
- website/cookies (where applicable).

Where we are required to supply data to funders/government (e.g., through specific programmes), we will ensure learners are signposted to the relevant privacy notices as part of enrolment (and we keep evidence that this has been provided).

12. Data minimisation, accuracy and quality

We ensure we only collect the personal data we need. We do this by:

- reviewing enrolment, exam and guidance forms regularly;

- avoiding “just in case” data collection;
- restricting free-text collection where a structured field is enough; and
- immediately correcting or securely deleting irrelevant personal data accidentally provided.

We take reasonable steps to keep data accurate, including:

- asking learners/staff to notify us of changes;
- updating records promptly when changes are received; and
- ensuring key decisions (e.g., exam entries, certificates) are based on verified information.

13. Records management, retention and secure disposal

We keep personal data **no longer than necessary** for the purpose(s) for which it was collected, including:

- educational and exam administration needs;
- legal and contractual obligations;
- audit/funding requirements where applicable; and
- safeguarding and dispute resolution needs.

13.1 Retention schedule and logs

Intech Centre maintains:

- a **Retention Schedule** (record type → retention period/rule → trigger event); and
- a **Retention & Destruction Log** (what was destroyed, when, how, and by whom).

13.2 Secure disposal (how we do it)

We dispose of personal data securely, including:

- **paper**: cross-cut shredding or secure confidential waste disposal;
- **electronic files**: secure deletion in line with IT controls;
- **devices/media**: secure wiping or physical destruction where wiping is not possible.

14. Information security and confidentiality

Intech Centre uses appropriate technical and organisational measures to protect personal data. Security is everyone’s responsibility.

14.1 Physical security

- Paper files containing personal data are stored in **locked cabinets/cupboards** with controlled access.
- Visitor access is managed to prevent unauthorised access to confidential areas.
- Screens displaying personal data (including CCTV monitors) are positioned to prevent viewing by unauthorised individuals.

14.2 IT and electronic security

- Access to systems is restricted to authorised users (role-based access where possible).
- Strong passwords are required and must not be shared.
- Devices must be locked when unattended.
- Personal data must not be stored on unapproved personal USB drives or unapproved cloud services.
- Where personal data must be transferred externally, secure methods are used (e.g., encrypted files or approved secure portals).

14.3 Off-site working

When working off-site:

- staff must prevent family/others from viewing confidential information;
- paper records must not be left unattended;
- loss/theft must be reported immediately to the Data Protection Lead.

15. Sharing personal data and disclosures

Intech Centre shares personal data only where:

- we have a lawful basis;
- the sharing is necessary and proportionate; and
- appropriate safeguards and security are in place.

15.1 Common sharing scenarios for Intech Centre

This may include sharing with:

- **awarding bodies / examination regulators** (exam registration, entries, adjustments, results, certification);
- **IT service providers** who host/support our systems (as processors, under contract);
- **professional advisers** (e.g., legal/accounting) where necessary;
- **authorities/safeguarding partners** where lawful and necessary (e.g., safeguarding concerns, serious incidents);
- **funding bodies/government** where required by funding/contract or law (where applicable).

15.2 Managing third-party requests

Any request for personal data from a third party (including family members, employers, police or other authorities) must be referred to the Data Protection Lead before disclosure, unless there is an immediate risk to life/safety and emergency escalation is required.

We do not sell personal data.

16. Processors, suppliers and contracts

Where a third party processes personal data on our behalf (a **processor**), we ensure:

- appropriate due diligence is conducted before onboarding;
- a written contract is in place containing UK GDPR required terms (processing instructions, confidentiality, security, sub-processor controls, breach notification, deletion/return at end of contract, audit rights); and
- the supplier is included on our supplier/processor register with review dates.

17. International transfers

If a supplier transfers personal data outside the UK (e.g., overseas hosting or support), Intech Centre will ensure:

- a lawful transfer mechanism and safeguards are in place; and
- transfer decisions are documented.

The DUAA introduces a new framing of the transfer test, including a "**not materially lower**" standard used in certain transfer assessments. Intech Centre will reflect this in transfer decision-making as the relevant provisions are commenced and guidance develops.

18. Individuals' rights

Individuals have rights under UK GDPR, including:

- **Right to be informed** (privacy notices);
- **Right of access** (Subject Access Request);
- **Right to rectification**;
- **Right to erasure** (limited circumstances);
- **Right to restrict processing** (limited circumstances);
- **Right to data portability** (where applicable);
- **Right to object** (including direct marketing);
- **Rights relating to automated decision-making/profiling** (where applicable);
- **Right to withdraw consent** (where processing relies on consent);
- **Right to complain to the ICO**.

Rights are subject to lawful exemptions and limitations.

19. Subject Access Requests (SARs) and other rights requests

19.1 How to make a request

Requests can be made:

- by email or in writing to the Data Protection Lead (contact in Section 28).

Any staff member receiving a request must forward it immediately to the Data Protection Lead.

19.2 Timeframe

We respond **without undue delay** and normally within **one month**, subject to lawful extensions where permitted.

19.3 Identity checks and clarification

We may request proof of identity where necessary to protect personal data.
If a request is unclear, we will ask for clarification promptly (for example: date range, course name, exam series, or specific documents sought).

19.4 DUAA SAR updates: "reasonable and proportionate searches" and "stop the clock"

ICO guidance explains DUAA changes to the right of access include:

- organisations only having to carry out a **reasonable and proportionate search**; and
- the ability to **"stop the clock"** when asking for clarification on a request, noting some changes may not yet be in force but are published to help organisations prepare.

Intech Centre will implement these approaches as applicable, and will:

- document our search plan and where searches were limited due to proportionality;
- document any "stop the clock" periods when awaiting clarification/required information.

19.5 Fees

We do not normally charge a fee. A fee will only be considered where permitted by law (e.g., manifestly unfounded or excessive requests) and any decision will be documented.

19.6 Redaction and third-party data

We will protect other people's personal data and apply redactions/exemptions where lawful and necessary.

19.7 Secure delivery

We will provide responses securely (e.g., encrypted attachments, secure portals, controlled collection with ID), depending on sensitivity and risk.

20. Data protection complaints process (DUAA)

ICO guidance for the public explains DUAA requires that organisations:

- take steps to help individuals make a complaint (e.g., provide an electronic complaints form);
- **acknowledge** the complaint **within 30 days**; and
- respond **"without undue delay."**

20.1 How to complain

Complaints can be submitted:

- by email to info@intechcentre.com (marked for the attention of the Data Protection Lead);
- in writing to the Intech Centre address; and
- via an electronic complaint form (available on request and/or via our website where provided).

20.2 What we will do

We will:

- acknowledge within 30 days;
- make appropriate enquiries and keep the complainant informed where resolution takes time;
- provide the outcome without undue delay;
- record the complaint, actions and outcome in the **Data Protection Complaints Log**.

If the complainant remains dissatisfied, they may complain to the **Information Commissioner's Office (ICO)**.

21. Marketing, communications, photos and testimonials

21.1 Marketing communications

Where Intech Centre sends marketing communications (e.g., course opportunities), we comply with UK GDPR and PECR. We ensure:

- clear opt-out options are provided; and
- opt-outs are respected and recorded.

21.2 Photos/testimonials/success stories

We will not use a learner's or staff member's image, name, video or testimonial for external promotional purposes unless we have an appropriate lawful basis and (where required) obtain **specific, recorded consent**. Consent can be withdrawn at any time. On withdrawal, we will stop future use and remove content where practicable (recognising that removal from third-party platforms may be limited by their systems).

22. Website cookies and storage/access technologies (PECR and DUAA)

Where Intech Centre operates a website, we provide a website privacy/cookie notice explaining what cookies are used and why, and how users can manage preferences.

ICO guidance describes exceptions to the usual rule requiring consent for storage/access technologies, including "strictly necessary" and "statistical purposes" exceptions, and explains updated rules following DUAA.

Intech Centre will:

- use "strictly necessary" cookies only where essential to provide a service requested by the user;
- provide transparency about cookies and similar technologies;
- collect consent where required; and
- where relying on an exception, provide clear information and (where required) an easy way to object.

23. CCTV

CCTV operates within Intech Centre for the purpose of protecting learners, staff, visitors and property.
We will:

- display clear signage explaining CCTV is in operation;
- restrict access to CCTV footage to authorised staff on a need-to-know basis;
- retain CCTV footage for a defined period and delete securely unless required for investigation;
- disclose CCTV footage only where lawful and necessary.

24. Automated decision-making and profiling

Intech Centre does not intend to make decisions about individuals that have legal or similarly significant effects solely by automated means without appropriate safeguards.
If we introduce automated decision-making in future (for example in admissions screening or exam integrity tools), we will:

- assess lawful basis and safeguards;
- carry out a DPIA where required; and
- provide transparency and enable appropriate review/challenge mechanisms.

25. Personal data breaches and incident response

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

All staff and contractors must report suspected breaches immediately to the Data Protection Lead.
We will:

- contain the incident and prevent further loss/disclosure;
- assess risk to individuals (including safeguarding risk);
- decide whether notification to the ICO and/or affected individuals is required;
- document the facts, effects and remedial action taken (including near misses) in the breach/incident log; and
- implement learning (training, process change, security improvements).

26. Training, awareness and culture

All staff will receive:

- data protection awareness training at induction; and
- refresher training at least annually (or sooner if significant changes occur).

Managers will ensure that staff understand:

- secure handling of learner/exam information;
- confidentiality expectations; and
- escalation routes for SARs, complaints and breaches.

Training completion is recorded in the training log.

27. Monitoring, audit and review

The Data Protection Lead will:

- review this policy annually (or sooner if required);
- monitor SAR, complaint and incident logs for trends and improvement actions;
- coordinate periodic checks on retention/disposal, access permissions and supplier contracts;
- ensure updates are communicated to staff and reflected in procedures.

Because DUAA provisions can be commenced in stages, Intech Centre will monitor ICO guidance and government commencement information and update procedures accordingly.

28. Contact details

Data Protection Lead / DPO contact: Salih Yilmaz, Senior Manager
Intech Centre: 362 Essex Road, Islington, London, N1 3PD
Telephone: 020 7354 5655
Email: info@intechcentre.com