Data Protection Policy

Author:	Compliance Manager
Contact details:	support@fledgetuition.com
Creation Date:	12th January 2020
Last Updated:	16th September 2025
Version:	0.5

1 Document Control

Change Record

Date	Author	Version	Change Reference
12th January 2020	Rory Tarabay	0.1	Initial draft
5th August 2021	Rory Tarabay	0.2	N/A - document review
26th August 2022	Rory Tarabay	0.3	N/A - document review
15th August 2023	Rory Tarabay	0.4	N/A - document review
16 September 2025	Laura Taylor	0.5	Updated to incorporate the Data (Use and Access) Act 2025 changes

Distribution

Name	Position
Arran Bayle	Co-Founder

Approval Sign-off

Name	Position	Date	Signature
Arran Bayle	Director	16/09/25	

2 Contents

3 Introduction

3.1 General

Fledge Tuition needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy seeks to ensure that Fledge Tuition:

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

This policy applies to every authorised person handling data. Whether a full-time member of staff or a freelancer, all are accountable for their actions and have a duty of care to ensure due diligence is afforded to data protection.

3.2 Data Protection Law

The Data Protection Act 2018 and the UK GDPR describe how organisations 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 law is underpinned by eight important principles; personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the United Kingdom unless the recipient jurisdiction or organisation provides an adequate level of protection or other lawful safeguards are in place.

These principles reflect the core UK GDPR principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality, and accountability.

The Data (Use and Access) Act 2025 (DUAA) received Royal Assent on 19 June 2025 and introduces targeted amendments to the UK GDPR, the Data Protection Act 2018 and PECR to promote responsible data use while preserving core protections. These changes are being phased in through 2025–2026.

DUAA changes affecting this policy:

- Introduces clarified / new lawful-basis rules (including a *Recognised Legitimate Interests* concept in defined circumstances);
- Changes handling of *Subject Access Requests* (SARs) — includes a "stop-the-clock" ability and a move to *reasonable and proportionate* search obligations (not exhaustive search);
- Amends rules around *Automated Decision-Making (ADM)* with specific safeguards and circumstances where some automated decisioning is permitted for non-sensitive data;
- Updates the Privacy and Electronic Communications Regulations (PECR) exceptions — in some low-risk cookie/ storage cases explicit consent requirements are relaxed;
- Modifies the test for some international transfers (a "data protection test") and gives the Secretary of State specified authorisation powers in limited scenarios.

3.3 Key Definitions

Personal Data refers to information about a living individual, which means that they can be identified (a) from that data, or (b) from that data and any other information which is, or could in the future, come into the possession of the data controller. Also see Special Categories of Personal Data.

Special Categories of Personal Data (also known as Sensitive Personal Data) refers to a specific sub-group of Personal Data, which comprises an individual's:

- racial or ethnic origin
- politics
- religion
- trade union membership
- genetics
- physical or mental health
- sexual preferences or activities

- biometric data (where used for ID purposes)

Data Controller refers to the person, organisation, public authority, agency or other body who, either alone or with others, determines the purposes for which and the manner in which any personal data is to be processed, and defines the controls required for such Processing.

Data Processor refers to any person or organisation (other than an employee of the Data Controller) who undertakes the Processing of personal data on behalf of the Data Controller.

Processing refers to any operation which is performed upon or applied to personal data, whether undertaken manually or by automated means, including its acquisition, organisation, storage, retrieval, consultation, amendment, availability, disclosure, erasure or destruction.

Data Subject refers to an individual who is the subject of personal data.

Data Subject Consent refers to the Data Subject's approval or agreement for an activity to take place, having given consideration to the benefits and risks of the activity. For consent to be valid, the data subject needs to be informed, have the capacity and knowledge to make a decision, and to have given their consent voluntarily.

Supervisory Authority refers to the national data protection authority of each relevant country. In the UK, the Supervisory Authority is the Information Commissioner's Office (ICO).

- **Recognised Legitimate Interests** — a DUAA-defined lawful basis applying in certain, limited circumstances (for example specified public interest or safeguarding contexts) where the statute identifies that processing is permitted without the same balancing test otherwise required under "ordinary" legitimate interests. Use of this basis must be strictly limited to the circumstances set out in DUAA and any applicable ICO guidance.

- **Automated Decision-Making (ADM)** — decision-making carried out by automated means. DUAA tightens the description of permitted ADM and the protections required where ADM produces legal or similarly significant effects; it also sets out circumstances where limited automated decisioning of non-sensitive data is permissible subject to safeguards (explanation, human review and appeals/right to challenge). Fledge Tuition will not rely on ADM for decisions producing significant legal effects without prior senior approval, DPO consultation, and documented safeguards.

---

4 Data Rights

4.1 Rights

Our policy is to:

Individuals have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;

- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for various purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the UK;
- object to decisions based solely on Automated Processing, including profiling (ADM), subject to the updated DUAA rules;
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.
- **Subject Access Requests (SARs):** DUAA introduces a **"stop-the-clock"** mechanism. This means that when we receive a SAR, we may pause the response deadline if we need additional information from the requester (for example to confirm identity, or to clarify/limit the scope). Once the requester supplies the necessary information, the response period resumes. Organisations must not use stop-the-clock to frustrate or deter requests and must keep clear records of any pauses.
- **Search scope for SARs:** The Act clarifies that controllers are required to perform **reasonable and proportionate searches** to satisfy SARs; exhaustive, disproportionate searches are not required. We must document our search approach and reasons for exclusions.
- **Automated Decision-Making (ADM):** While the fundamental right to object to ADM remains, DUAA clarifies circumstances where some automated processing of non-sensitive data is permissible if robust safeguards (meaningful explanation, human oversight and an effective challenge route) are in place. Fledge Tuition will continue to treat ADM cautiously and will not rely on any new DUAA-permitted automated decisioning unless the safeguards are demonstrably implemented.
- **Complaints:** DUAA and associated guidance emphasise accessible complaint channels. Individuals now have a formal right to submit complaints electronically and to be informed of complaint outcomes; our complaints procedure will record and respond to electronic complaints in the same timely way as other complaints. Staff should log and escalate all complaints (including electronic) through the designated procedure.

5 Practical changes Fledge Tuition will implement

The following operational steps are mandatory for compliance and good practice:

1. **Privacy Notice updates** — update all privacy notices and fair-processing information to:
    - reflect any use of *Recognised Legitimate Interests* and the legal basis relied upon;
    - explain any use of ADM and the safeguards in place;
    - identify lawful bases and any international transfers and safeguards.

2. **Subject Access Request (SAR) procedure** — update SAR templates and staff guidance to:
    - implement the “stop-the-clock” process (record when a clock is paused and why);
    - apply proportionate search procedures and maintain evidence of scope decisions;
    - ensure responses are still timely once clarification or identity verification is received.

3. **ADM / Profiling controls** — before deploying or continuing automated decision systems, complete an ADM assessment that documents: legal basis, likelihood of significant effect, safeguards (human review, explanation, appeals route), DPIA results where required. Do not deploy ADM relied on the new DUAA allowance without the documented safeguards.

4. **Cookies & PECR** — review website cookie notices and consent mechanisms: for low-risk functional/analytics cookies where DUAA/PECR guidance permits, ensure the new permitted use is documented and that users are still properly informed and given meaningful choice for tracking/advertising cookies. Review ICO updated guidance and implement any required changes to banners or settings.

5. **International transfers** — review existing transfer mechanisms (adequacy decisions, SCCs, BCRs, or other safeguards). Under DUAA the “equivalence” requirement is supplemented by a “data protection test” approach in some cases; where we rely on newly permitted transfer routes we will document the legal basis and any Secretary of State authorisations where applicable.

6. **Training & record-keeping** — update staff training to explain the DUAA amendments (SAR changes; ADM safeguards; cookie/PECR updates; transfer test) and keep records of decisions under the changed regime.

7. **Breach / DPIA processes** — maintain DPIAs for higher-risk processing and continue to report notifiable breaches to the ICO as required by law. Keep DPIA documentation and breach logs up to date to show compliance.

If you receive a request to enact a data subject right

If you receive a request to enact any of the rights listed above, you must **immediately** send an email with the details to your line manager and the DPO (where applicable). This ensures that we do not allow third parties to persuade you into disclosing or deleting Personal Data without proper authorisation and enables timely, documented handling (including applying the "stop-the-clock" if more information from the requester is legitimately required).

---

6 Review, governance and next steps

- This policy will be reviewed and updated as ICO guidance on DUAA is published and refined (ICO has stated it will publish updated guidance in phases through 2025–2026).
- The DPO (or designated privacy lead) will prepare a short implementation plan and staff briefing within 30 days of this version to ensure Fledge Tuition meets the new operational requirements.