Data Protection Policy

FUTURES-ESSEX

EDUCATING MINDS, SOARING HIGH

Approved by:	Lauren Collin	**Date:**	16 April 2024
Last reviewed on:	1st August 2025		
Next review due by:	1st August 2026		

1. Aims

Futures-Essex Ltd aims to ensure that all personal data collected about staff, pupils, parents and carers, directors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative Artificial Intelligence in Education.

Biometric data: Futures-Essex Ltd does not collect and is not reliant on biometric data. If applied in the future, the policy will meet the requirements of the Protection of Freedoms Act 2012.

CCTV data: Futures-Essex Ltd does not use CCTV. If applied in the future, the policy will reflect the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. It also complies with our funding agreement and articles of association.

3. Definitions

Personal data: Any information relating to an identified, or identifiable, living individual (name, ID number, location data, online identifier, etc).

Special categories of personal data: Sensitive data such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetics, biometrics (where used for ID), health, sex life or sexual orientation.

Processing: Anything done to personal data, automated or manual.

Data subject: The individual whose data is held.

Data controller: The organisation determining purposes and means of processing.

Data processor: A person or body processing personal data on behalf of the controller.

Personal data breach: A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data.

4. The data controller

Futures-Essex Ltd processes personal data relating to parents, carers, pupils, staff, directors, visitors and others, and is a data controller.

The organisation is registered with the ICO and has paid its data protection fee (ICO Registration Number: ZB681034).

5. Roles and responsibilities

This policy applies to all staff employed by Futures-Essex Ltd, and to external organisations/individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Directors: overall responsibility for ensuring compliance with data protection obligations.

5.2 Data Protection Officer (DPO): Michael Bradbrook. Responsible for overseeing implementation, monitoring compliance, reporting annually, and being the first point of contact for individuals and the ICO.

5.3 Provision Manager: represents the data controller day to day.

5.4 All staff: responsible for correct data collection, storage and processing, informing the facility of changes to their data, and contacting the DPO in case of queries, breaches, or uncertainty about lawful bases, consent, privacy notices, contracts, or transfers outside the UK.

6. Data protection principles

The UK GDPR principles require data to be:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit, legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept no longer than necessary
- Processed securely

This policy explains how Futures-Essex Ltd complies with these principles.

7. Collecting personal data

We process data only where lawful, fair and transparent. Lawful bases include contract fulfilment, legal obligation, vital interests, public interest, legitimate interests, and consent.

Special category data requires additional conditions (e.g. explicit consent, employment law, health/social care, public interest). Criminal offence data requires both a lawful basis and condition.

We always consider fairness and individuals' reasonable expectations.

Staff must only collect necessary data, keep it accurate and up to date, and delete/anonymize when no longer required (in line with the retention schedule).

8. Sharing personal data

We do not normally share personal data without consent, except where required (e.g. safeguarding, safety, legal obligation, emergency response).

Suppliers and contractors are only engaged with proper data protection guarantees and contracts. We may share data with law enforcement/government where required, and emergency services when necessary.

International transfers are only made in line with UK data protection law.

9. Subject access requests and other rights

Individuals have the right to access their personal data. Requests may be made in any form, but written requests help us respond quicker. Staff must forward any request to the DPO immediately.

Children's rights: Under 12s are generally not mature enough to exercise rights themselves, so

parental requests may be granted. Over 12s are generally regarded as mature enough, so parental requests usually need the pupil's consent. Judgement is case-by-case.

We respond without delay, within 1 month, free of charge (or within 3 months for complex cases). Information may be withheld where disclosure could cause harm, reveal third-party data, or fall under legal exemptions.

Other rights include rectification, erasure, restriction, objection, portability, withdrawal of consent, objection to automated decision-making, and being informed of breaches.

10. Parental requests

Parents (or those with parental responsibility) may request access to their child's educational record within 15 days. In academies/independent schools there is no automatic right, but requests are reviewed case by case at Futures-Essex. Fees may apply for copies. Requests may be denied where disclosure may cause harm or contravene exam result rules.

11. Biometric recognition systems

Futures-Essex Ltd does not use biometric systems. If introduced, it will comply with the Protection of Freedoms Act 2012.

12. CCTV

Futures-Essex Ltd does not use CCTV. If introduced, it will comply with ICO guidance on surveillance cameras.

13. Photographs and videos

Written consent will be obtained from parents/carers (or pupils aged 18+) for photographs/videos used for communication, marketing or promotional purposes. Uses include displays, publications, social media, websites. Consent can be withdrawn at any time. Photos/videos will not include identifying personal information. Parents taking photos for personal use at events are asked not to share publicly without consent from others involved.

14. Artificial Intelligence (AI)

AI tools (e.g. ChatGPT, Bard) must not be used to input personal or sensitive data. Doing so will be treated as a data breach and handled under Appendix 1.

15. Data protection by design and default

Measures include appointing a qualified DPO, conducting impact assessments, embedding data protection into policies and training, keeping processing records, and ensuring safeguards for international transfers.

16. Data security and storage

We protect data by physical and digital safeguards. Examples: locked storage, encrypted portable devices, 10+ character passwords, no password reuse, due diligence for third-party sharing, acceptable use rules for personal devices.

17. Disposal of records

Data is securely destroyed when no longer needed (e.g. shredding, deletion, certified third-party disposal).

18. Personal data breaches

Breaches will be reported to the DPO (Michael Bradbrook) immediately. The DPO will investigate, mitigate, and notify ICO within 72 hours if required. Individuals affected will be informed. All breaches will be documented, trends reviewed, and lessons learned implemented.

19. Training

All staff and Directors receive training on induction and as part of continuing professional development. Updates are provided when law or policy changes.

20. Monitoring arrangements

The DPO monitors compliance and reviews this policy annually. It is approved by the Directors.

21. Links with other policies

This policy links to: Freedom of Information publication scheme, Privacy notices, Online safety policy, ICT Acceptable Use policy, Safeguarding policy, Bring Your Own Device (BYOD) policy, and others as relevant.

Appendix 1

Personal Data Breach Procedure:

- Staff must report breaches immediately to the DPO (Michael Bradbrook).
- The DPO investigates, contains, assesses risks, and documents the breach.
- ICO notified within 72 hours if required.
- Affected individuals informed in plain language where required.
- Records of breaches are stored securely.
- The DPO and Provision Manager meet monthly to review breaches and identify patterns.
- Example mitigations include recalling mis-sent emails, contacting recipients to delete data, removing published information, involving safeguarding leads, and liaising with third parties (e.g. banks, insurers, police) if necessary.