Data Protection Policy

Title	Data Protection Policy
Author/Owner	IGS, Essex County Council (C3 2024)
Status	Final - Approved
Ratified Date	September 2024
Ratified by	Audit and Risk Committee
Staff Consultation Date	N/A
Review Cycle	Annual
Review Date	June 2025
Security Classification	OFFICIAL

Data Protection Policy

Data Protection is a legal requirement and is vitally important for ensuring that the data of pupils, parents/carers, and those that work with Discovery Educational Trust (DET) and its Schools is kept secure. This protects the rights of individuals, and ensures that the risks of data processing are well managed.

This Policy details the rules that all staff, contractors and volunteers **must** follow when processing personal data.

Policy Rules

1. All employees must **comply** with the requirements of Data Protection law and Article 8 of the Human Rights Act when processing the personal data of living individuals.
2. Where personal data is used, DET/its Schools must ensure that the Data Subjects have access to a complete and current **Privacy Notice.**
3. DET and its Schools must formally **assess** the risk to privacy rights introduced by any new (or change to an existing) system or process, which involves the use of personal data.
4. DET and its Schools must process only the **minimum** amount of personal data necessary to deliver services.
5. All employees, who record **opinions** or intentions about pupils, parents/carers or staff must do so carefully and professionally.
6. DET and its Schools must take reasonable steps to ensure that the personal data held is **accurate**, up-to-date and not misleading.
7. DET and its Schools must rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition.
8. Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services.
9. Consent **expires** at the end of each 'Key Stage' period, unless it is reconfirmed.
10. DET and its Schools must ensure that the personal data processed is reviewed and **destroyed** when it is no longer necessary.
11. If DET and its Schools receive a **request** from a member of the public or colleague asking to access their personal data, the request must be managed as a Subject Access Request under the Data Protection Act 2018 or a request for the Education Record under the Education (Pupil Information) (England) Regulations 2005.
12. If DET/its Schools receive a request from anyone asking to access the personal data of **someone other than themselves**, Data Protection law must be fully considered before disclosing it.
13. When someone contacts DET/its Schools requesting changes to the way in which we process their personal data, DET/its Schools must fully consider their **rights** under Data Protection law.

14. You must not access personal data, which you have **no right to view.**
15. You must follow system user **guidance** or other formal processes. which are in place to ensure that only those with a business need to access personal data are able to do so.
16. You must only **share** personal data with external bodies that request it if there is a current agreement in place to do so or it is approved by the Data Protection Officer (DPO) or Senior Information Risk Owner (SIRO).
17. Where the content of telephone calls, emails, internet activity and video images of employees and the public is **recorded, monitored and disclosed,** this must be done in compliance with the law and the regulator's Code of Practice.
18. All employees must be **trained** to an appropriate level, based on their roles and responsibilities, to handle personal data securely. This training must be regularly refreshed to ensure that knowledge remains current.
19. When using **'data matching'** techniques, this must only be done for specific purposes in line with formal codes of practice, informing pupils, parents/carers or staff of the details, their legal rights and obtaining their consent, where appropriate.
20. DET must pay an annual Data Protection Fee.
21. Where personal data needs to be anonymised or pseudonymised, for example, for **research purposes**, DET and its Schools must follow the relevant procedure.
22. You must not **share** any personal data held by the Trust/School with an individual or organisation based in any country outside of the United Kingdom without seeking advice from the SIRO or Data Protection Officer.
23. DET and its Schools must identify **Special Categories** of personal data and ensure that it is handled with appropriate security, and only accessible to authorised persons.
24. When **sending** Special Category data to an external person or organisation, it should be marked as "OFFICIAL-SENSITIVE" and, where possible, sent by a secure method.
25. When considering the use of **artificial intelligence** involving the use or creation of personal data, you can only do so with the approval of the DPO and the SIRO.

How must I comply with these Policy Rules?

DET and its Schools have related policies, procedures and guidance, which assist staff in ensuring compliance with these rules. These include:

- Statutory Requests Policy;
- Data Handling Security Policy;
- Data Breach Policy;
- Records Management Policy;
- Biometrics Policy (if used by the School);
- Generative Artificial Intelligence Policy (if used by the School);
- Privacy Notice Procedure;
- Data Protection Rights Procedure;
- Publishing for Transparency Procedure;
- Consent Procedure;
- Minimisation of Personal Data Procedure;

- Data Breach Procedure;
- Data Sharing Procedure;
- Subject Access Request Procedure;
- Marketing Procedure;
- Surveillance Procedure;
- Retention Schedules;
- Training and Awareness Procedure;
- Statutory Requests for Information Guidance;
- Overseas Transfers and Hosting Guidance.

If you are unsure about how to comply, you must seek advice and guidance from your Data Protection Lead/School Business/Office Manager.

What if I need to do something against this Policy?

If you believe that you have a valid business reason for an exception to these Policy Rules, having read and understood the reasons why they are in place, please raise a formal request by contacting the HT/SIRO on the below School email addresses:

- Chase High School – gdpr@chasehigh.org;
- Hogarth Primary School – gdpr@hogarth.essex.sch.uk;
- Kelvedon Hatch Community Primary School – gdpr@kelvedonhatch.essex.sch.uk;
- Larchwood Primary School – gdpr@larchwood.essex.sch.uk;
- St. Martin's School – gdpr@st-martins.essex.sch.uk.

References

- Data Protection Act 2018/UK GDPR;
- Article 8, The Human Rights Act 1998;
- Education (Pupil Information) (England) Regulations 2005;
- Investigatory Powers Act 2016.

Breach Statement

Breaches of Information Policies, of which this Policy is one, are thoroughly investigated and may result in disciplinary action. Serious breaches of policy may be considered as gross misconduct and result in dismissal without notice, or legal action being taken against you.