Data Protection Policy

Title	Data Protection Policy
Author/Owner	IGS, Essex County Council (C3 2023)
Status	Final - Approved
Ratified Date	November 2023
Ratified by	Audit and Risk Committee
Staff Consultation Date	N/A
Review Cycle	Annual
Review Date	October 2024
Security Classification	OFFICIAL

Data Protection Policy

This Policy details general rules for Discovery Educational Trust and its School in complying with Data Protection law.

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' in further sections.

What must I do?

1. ***MUST***: 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. ***MUST***: Where personal data is used, DET/its Schools must ensure that the Data Subjects have access to a complete and current **Privacy Notice.**
3. ***MUST:*** DET/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. ***MUST***: DET/its Schools must process only the **minimum** amount of personal data necessary to deliver services.
5. ***MUST***: All employees, who record **opinions** or intentions about pupils, parents/carers or staff, must do so carefully and professionally.
6. ***MUST***: DET/its Schools must take reasonable steps to ensure that the personal data they hold is **accurate**, current and not misleading.
7. ***MUST***: DET/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. ***MUST***: Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services.
9. ***MUST***: Consent **expires** at the end of each 'Key Stage' period, unless it is reconfirmed.
10. ***MUST***: DET/its Schools must ensure that the personal data they process is reviewed and **destroyed** when it is no longer necessary.
11. ***MUST***: If DET/its Schools receive a **request** from a member of the public or colleagues asking to access their personal data, they must handle it 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. ***MUST***: If DET/its School receive a request from anyone asking to access the personal data of **someone, other than themselves**, they must fully consider Data Protection law before disclosing it.
13. ***MUST***: When someone contacts DET/its Schools requesting that DET/its Schools change the way their personal data is processed, DET/its Schools must consider their **rights** under Data Protection law.
14. ***MUST NOT***: You must not access personal data, which you have **no right to view.**
15. ***MUST***: 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. ***MUST***: You must **share** personal data with external bodies, who request it, only 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. ***MUST***: 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. ***MUST***: All employees must be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely. This training must be regularly refreshed to ensure that knowledge remains current.
19. ***MUST***: 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 getting their consent, where appropriate.
20. ***MUST***: We must pay an annual Data Protection Fee.
21. ***MUST:*** Where personal data needs to be anonymised or pseudonymised, for example for **research purposes**, DET/its Schools must follow the relevant procedure.
22. ***MUST NOT***: You must not **share** any personal data held by DET/its Schools with an individual or organisation based in any country outside of the United Kingdom without seeking advice from the DPO or SIRO.
23. ***MUST***: DET/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. ***MUST***: 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.

Why must I do it?

1. To comply with legislation.
2. To comply with Data Protection Law, which requires DET/its Schools to make the Data Subject aware of how their personal data is handled.
3. To ensure that the rights of the Data Subject are protected in any proposed new activity, or change to an existing one.
4. The law states that DET/its Schools must only process the minimum amount of information needed to carry out their business purpose. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate.
5. To maintain professional standards and to assist in defending the validity of such comments if the Data Subject exercises their rights to ask DET/its Schools to amend or delete their personal data if they feel it to be inaccurate.
6. To comply with a principle of Data Protection law.
7. To comply with Data Protection law, where processing does not rely on a legal condition other than consent.
8. When using personal data for marketing and promoting services, it is unlikely that any lawful condition other than consent would apply.
9. Consent can only be valid for a reasonable period of time.
10. To comply with a principle of Data Protection law.
11. To comply with the right to access personal data.
12. To comply with a principle of Data Protection law.
13. To comply with the rights of the Data Subject under Data Protection law.
14. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so.

15. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so.
16. To comply with the legal requirements to keep personal data secure, but also to ensure that, where there are legal grounds to share information in a managed way, this is done correctly.
17. The law permits organisations to hold such data in order to measure the quality of services being provided, to record consent etc. In certain circumstances, recordings may be accessed, for example, to investigate alleged criminal activity or breaches of DET/School policy etc.
18. To comply with a principle in Data Protection law, regulatory guidance and the DPO governance requirements.
19. To comply with the Data Subject's rights.
20. This is a regulatory requirement.
21. Where personal data is used for research purposes, the processing of the data can be legitimised by provisions within Data Protection law.
22. To comply with the right of the Data Subject to have equivalent legal safeguards in place over their data in another country as they would in the UK. Personal data transferred overseas (including hosted solutions) must be securely handled under the same, or substantially similar, provisions that exist under the Data Protection Act.
23. To comply with Article 9 of General Data Protection Regulations (GDPR).
24. To comply with Article 9 of GDPR and comply with a principle of Data Protection law requiring that personal data is processed with appropriate security measures.

How must I do it?

1. By following the points in this Policy.
2. By approving and reviewing a compliant Privacy Notice in line with the Privacy Notice Procedure and making it available to the Data Subjects.
3. By completing and approving a Privacy Impact Assessment, or Data Protection Impact Assessment where the processing is 'high risk' to the rights of the Data Subjects.
4. By ensuring that the means that DET/its Schools use to gather personal data (such as forms etc.) only ask for the information that is required in order to deliver the service.
5. By considering that anything committed to record about an individual may be accessible by that individual in the future, or challenged over its accuracy.
6. For example, there should be, at least, an annual check of the currency of data held about pupils, parents/carers or staff, and whenever contact is re-established with them, DET/its Schools should check that the information they hold about them is still correct.
7. By following the points in the DET Consent Procedure.
8. By following the points in the DET Consent Procedure.
9. By following the points in the DET Consent Procedure. Parents/carers of pupils in the last year of a Key Stage should expect a communication to ask them to refresh their consents. If they do not respond ahead of a deadline date, consent should be assumed to be no longer valid.
10. By following the points in the DET Records Management Policy. DET/its Schools must review personal data regularly and delete information, which is no longer required; although DET/its Schools must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the law allows DET/its Schools to keep indefinitely personal data processed only for historical, statistical or research purposes. The DET Retention Schedules provide guidance in these areas.

11. By following the points in the DET Statutory Requests for Information Policy. DET/its Schools must be aware that Data Subjects can ask others to make a request on their behalf. There must be evidence of consent provided by the Data Subject to support this.
12. By following the points in the DET Statutory Requests for Information Policy. Such requests would, typically, be managed under the Freedom of Information Act (if from a member of the public) or under Data Protection or Justice law (if for a criminal investigation). However, the decision whether or not to disclose someone's personal data to a third party must satisfy the requirements of Data Protection law.
13. By reviewing the impact of any requested change on any statutory duty being fulfilled by DET/its Schools.
14. By being aware, through training and guidance from your Line Manager, of what information is appropriate for you to access to do your job. Systems and other data storage must be designed to protect access to personal data. You must inform your Line Manager if you have access to data, which you suspect that you are not entitled to view.
15. By ensuring appropriate security controls are in place, and rules to support those controls are followed. The following should be in place:
    - technical methods, such as encryption, password protection of systems, restricting access to network folders;
    - physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure; and
    - organisational measures, such as:
        - Providing appropriate induction and training so that staff know what is expected of them;
        - Taking reasonable steps to ensure the reliability of staff that access personal data, for example, by the use of Disclosure and Barring Service (DBS) checks;
        - Ensuring that passwords are kept secure, forced to be changed after an agreed period, and are never shared.
16. Consult your Line Manager, any procedural guidance or any library of sharing agreements managed by DET/its Schools. Consult the DPO or SIRO in one-off cases of sharing.
17. By ensuring that employees and members of the public are fully aware of what personal data is being recorded about them and why, and in what circumstances that data may be used. Operation of overt surveillance equipment such as CCTV must always be done in line with relevant Codes of Practice captured in the DET Surveillance Management Procedure. Any covert surveillance must be done in line with the provisions in the Investigatory Powers Act (2016).
18. By completing compulsory training courses relevant to your role. Records are kept of induction training and annual refresher training. Training content for each role is determined by feedback on current training methods and the outcome of investigating data breaches. This is reviewed frequently.
19. By ensuring that an Impact Assessment has been approved for the activity.
20. The payment must be made annually to the Information Commissioner's Office (ICO).
21. Follow the guidance in the DET Minimisation of Personal Data Procedure.
22. Consult the DPO over any proposed sharing outside of the UK. If you are a Line Manager, who is proposing a change to, or implementing, a new system, which may involve the hosting of personal data in a nation outside of the UK, this must be first assessed by a Privacy Impact Assessment, which must be approved by your DPO and your SIRO.
23. Special Categories of Personal Data are information revealing *racial or ethnic origin*, *political opinions*, *religious or philosophical beliefs*, or *trade union membership*, and *genetic data*, *biometric data* for the purpose of uniquely identifying an individual, *data concerning health* or *data concerning an individual's sex life or sexual orientation*. This data should be stored securely and in a way that access is restricted only to those members of staff that have a valid need to access it. It should only be shared externally after verifying that the recipient is entitled to access this data, and through secure means.

24. Hard-copy packages must be marked as such by writing on the exterior of the package. Emails should contain the wording in the 'subject' field before the email title. Refer to the Records of Processing Activity document and the register of Data Flows for clear instruction on how you are expected to handle sending the data securely according to the particular activity that you are undertaking.

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 points, having read and understood the reasons why they are in place, please raise a formal request by contacting the Headteacher/SIRO on the below DET School email addresses:

- Chase High School – gdpr@chasehigh.org;
- Hogarth Primary School – gdpr@hogarth.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 (including the 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 are investigated and may result in disciplinary action. Serious breaches of policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.