Data Protection Strategy

This strategy and accompanying policies are in place to ensure all staff and those responsible for governance are aware of their responsibilities and outlines how the Trust complies with the core principles of the GDPR.

Version number	5.1
Approved by	Board of Trustees
Approval date	May 2020
Adopted by	n/a
Adopted date	n/a
Implementation date	November 2020
Policy/document owner	Director of Operations
Status	Statutory
Frequency of review	Every three years
Next review date	June 2023
Applicable to	This policy applies to the Trust and all constituent schools.

Document History

Version	**Version Date**	Author	Summary of Changes
V1.0	25.02.2018	Director of Operations	New strategy – 1st Draft
V2.0	27.03.2018	Director of Operations	Revised Policy following comments of CEO
V3.0	16.04.2018	Director of Operations	Reviewed with Director of IT
V4.0	01.05.2018	Director of Operations	Reviewed Governance structures
V5.0	May 2020	Head of Governance	Reviewed by Executive Team. Changes to general wording, formats and ordering of information. Additional sections added on responsibilities, storing personal data, procedure for responding to rights request and training.
V5.1	November 2020	Head of Governance	Updated branding

Contents

1. Aims

Discovery Schools Trust is a single legal entity, therefore references to "the Trust" in this strategy should be considered as inclusive of its schools.

The Trust aims to ensure that all data collected about staff, pupils, parents, governance volunteers and visitors is collected, stored and processed in accordance with the Data Protection Act 1998 and the General Data Protection Regulations (GDPR).

The Trust collects and uses certain types of personal information in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding.

This strategy and related policies apply to all data, regardless of whether it is in paper or electronic format.

Responsibilities

2. Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations. The Board of Trustees has delegated operational responsibility for data protection to the Director of Operations.

3. Trust Responsibilities

The Trust processes personal information relating to pupils, staff, volunteers and visitors, and, therefore, is the **data controller**.

The Trust is responsible for:

- establishing data protection policies and procedures in addition to demonstrating compliance with data protection law;
- appointing a suitably qualified Data Protection Officer;
- providing comprehensive, clear and transparent privacy policies;
- quality assuring internal data protection activities
- reporting to the Board of Trustees annually on the effectiveness of the strategy.

Responsibility for the day to day data management is delegated to the Local Data Protection Representatives (LDPR) and Headteacher or relevant senior leader at each school/workplace location.

4. Data Protection Officer (DPO) responsibilities

The Flying High Trust will act as the organisation's DPO and will work with the Director of IT and the Director of Operations. The DPO main responsibilities are:

- advising the organisation of their obligations under GDPR;
- monitoring the organisation's compliance with the GDPR and other relevant data protection laws.

5. Headteachers and Trust Line Managers

The Headteacher of each school will act as the representative of the data controller on a day-to-day basis and will ensure the Local Data Protection Representative has the time and resources to undertake the role.

6. Local Data Protection Representatives (LDPR)

The nominated LDPR in each workplace location will be:

- Schools - Office Manager
- Central Services - Director of Operations

Local Data Protection Representatives (LDPR) have operational responsibility for day-to-day data management and championing data protection in their location. They will:

- work with the Director of Operations to ensure that all staff are aware of their data protection obligations;
- oversee the local management of data protection including the storage, processing and retention of personal data;
- seek advice on data protection queries from the Director of Operations;
- report any data protection breaches to the Director of Operations within the required timescales and support their resolution; and will
- be the first point of contact on all data protection matters and provide advice and information to local staff.

7. All staff

Staff members who process personal data must comply with the requirements of this strategy and related policies. Staff members must ensure that:

- all personal data is kept securely and processed in line with policy;
- they only process personal data where it is necessary in order to do their jobs.
- personal data is not disclosed to any unauthorised third party. Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the LDPR.
- personal data is kept in accordance with the retention schedule. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised in accordance with the Trust retention schedule.;
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the LDPR in the first instance;
- data protection breaches are swiftly brought to the attention of the Local Data Protection Representative and that they support the investigation and resolution of a breach; and
- changes to their personal data, such as a change of address are notified to their workplace.

8. Contractors, Short-Term and Voluntary Staff

All practical and reasonable steps must be taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

The Trust is responsible for the use made of personal data by anyone working on its behalf.

Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing.

Contractors and volunteers must be made aware of their work responsibilities in relation to personal data and adhere to this strategy.

Key principles

9. Personal data protection principles

The Trust commits to processing all personal data in compliance with the data protection principles (unless a data protection law exemption applies).

<table>
<tr><td colspan="2">Processing of personal data must be lawful, fair and transparent</td></tr>
<tr><td rowspan="5">Personal data must be</td><td>Collected for specified, explicit and legitimate purposes</td></tr>
<tr><td>Adequate, relevant and limited to the purposes it is being used for</td></tr>
<tr><td>Accurate and kept up to date</td></tr>
<tr><td>Kept for no longer than necessary</td></tr>
<tr><td>Kept safe and secure</td></tr>
<tr><td colspan="2">As the Data Controller, the Trust is responsible for, and must be able to demonstrate compliance with these principles</td></tr>
</table>

This strategy sets out how the organisation aims to comply with these principles.

10. Lawful processing

The Trust must have a valid lawful basis (legal reason) to process personal data. We will only process data where we can identify at least one of the six legal reasons:

- the data needs to be processed so the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract;
- the data needs to be processed so that the Trust can **comply with a legal obligation**;
- the data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life; or emergency situation;
- the data needs to be processed so that the Trust, as a public authority, can perform a task in the **public interest**, and carry out its official functions;

- the data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden);
- the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law set out in a **privacy notice**.

11. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- we need to liaise with other agencies – we may need to seek consent as necessary before doing this;
- our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies, educational and operational software providers. When doing this, we will:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - establish a data sharing agreement with the supplier or contractor, either in the contract or as a stand-alone; agreement, to ensure the fair and lawful processing of any personal data we share;
    - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- the prevention or detection of crime and/or fraud;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax owed to HMRC;
- in connection with legal proceedings;
- where the disclosure is required to satisfy our safeguarding obligations;
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

12. Consent

In certain circumstances we will use consent as a legal basis for processing personal data (only where none of the other basis apply - see section 10). Examples include using names, photos, videos or

other identifying information about a pupil on a school's website, newsletter, or other promotional material.

We will ensure that consent mechanism we use meet the standards of the GDPR a record will be kept documenting how and when consent was given.

The consent statement will make it clear that it may be withdrawn by the individual at any time.

Rights of individuals

Under data protection law, individuals have rights with regards to their information. We will publish information about how individuals can exercise these rights on our website.

13. The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This includes the purposes for processing their personal data, the retention periods for that personal data, and details of who it will be shared with. The right to be informed is covered by our published **Privacy notice.**

14. The right to access (Subject Access Requests)

The right to access is also known as a "Subject Access Request" (SAR).

Individuals have the right to receive a copy of their personal data which is held by the Trust. This relates to any data held on computer, electronic or in manual record systems.

Some data may be exempt from disclosure; the Trust will inform the individual where data has been withheld due to it being the subject of an exemption.

If staff identify a subject access request they must immediately report it to their LDPR.

The **GDPR Data Subject Access Rights Procedure** outlines the steps that will be followed on receipt of a SAR.

15. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data corrected. We will take reasonable steps to check the accuracy of the data and to rectify it if necessary.

Where the data has been disclosed to a third party, we will inform them of the rectification where possible. Where appropriate, we will inform the individual about the third parties that the data has been disclosed to.

16. The right to erasure ('right to be forgotten')

Individuals have the right to request the deletion or removal of personal data under certain circumstances.

We can refuse a request where the data is required to comply with a legal obligation or claim, or where the data is required for purposes relating to public health.

We will inform any third parties with which the data had been shared, unless doing so is impossible or is unlikely to be effective.

17. The right to restrict processing

Individuals have the right to block or suppress the processing of personal data where the accuracy of the data is contested, or the data has been unlawfully processed.

We will restrict processing until the data has been corrected or until we have confirmed that the data is accurate.

Where no grounds for restriction are found, the individual will be notified that the restriction will be lifted.

In the event that processing is restricted, sufficient personal data will be stored about the individual to ensure that the restriction is respected in future.

If the data was provided to a third party, we will inform that party of the restriction, unless doing so is not possible or not likely to be effective. We are not under any obligation to make sure that the third party does not further process it.

18. The right to data portability

The right to data portability allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data that an individual has personally provided to the Trust
- where the processing is based on consent or the performance of a contract
- where processing is carried by automated means (i.e. excluding paper files)

A request may be refused against the grounds set out in the GDPR.

Where a request is granted, it will be shared in a commonly used and machine-readable form at no cost. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

19. The right to object

There is no right for an individual to object to processing in general, however individual do have a right to object to:

- Processing which is for direct marketing purposes
- Processing for scientific/historical research/statistical purposes
- Processing for a task in the public interest/legitimate interests.

A request to object to data processing will be validated against the conditions set out in the GDPR.

Where an objection is valid, we will stop processing the personal data of the individual.

A request may be refused where there is a compelling legitimate ground for processing the personal data or where it is required for a legal claim.

20. Rights in Relation to Automated Decision Making and Profiling

Automated decision-making takes place when an electronic system uses personal information to make decisions without human intervention.

Individuals have the right not to be subject automated decision-making, including those based on profiling, that have a legal or similarly significant effect on individuals.

At present, there are no fully automated decision making or profiling systems in use within the Trust. This means that this right does not currently apply to any processing activities.

21. Procedure for responding to rights requests

We will publish information about how individuals can exercise their rights on the Trust website.

The **GDPR Data Subject Rights Procedure** outlines the process that will be followed on receipt of a rights request in relation to (see attached annex):

- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object

The right to be informed is covered by our published **Privacy notice.**

The subject access right is covered by our **GDPR Data Subject Access Procedure** (see attached annex).

Rights requests will be responded to within one month; this will be extended by two months where the request is complex.

We can request a "reasonable fee" or deny a request if it can be justified that the request was unfounded or excessive.

Where no action is being taken in response to a request, we will explain the reason for this to the individual and will inform them of their right to complain to the ICO.

If there is a fee, the request will not be actioned until the fee has been received.

Demonstrating Accountability

22. Data protection impact assessments (DPIA)

The Trust will consider carrying out a DPIA for any major project involving the use of personal data. The DPIA process is covered under separate guidance.

The responsibility for carrying out a DPIA lies with the individual responsible for the project or service involved.

An initial screening will be completed to decide if a DPIA is required. A DPIA Initial Screening Template is available in the attached annex.

23. Data breach

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All reasonable endeavours will be made to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set in the **Data Breach Policy and Process** document.

The Director of Operations will ensure that LDPR's cascade information to all staff members, to ensure they are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

24. Data security and storage of records

We will put in place measures to maintain data in a safe, secure and confidential manner, including but not restricted to:

- Control of access to data - access to personal data is on a 'need to know' basis.

- Implementation of physical controls e.g CCTV, access control, secure storage
- Implementation of technical controls e.g encryption, firewalls, password protection
- Protection controls to secure email, documents, and sensitive data shared outside the Trust
- Ensure high staff awareness e.g staff training – how to keep data secure, data minimisation, update records promptly, secure password principles
- Ensure confidential disposal of documents e.g. shredding facilities
- Ensure periodic checks of security measures and implement measures where gaps are identified
- Ensure procedure in place for dealing with data breaches

The **Director of Operations** and **Director of IT** are responsible for ensuring that continuity and recovery measures are in place to safeguard the security of protected data.

25. Publication of information

The Trust publishes key statutory requirements on its website outlining different types information that will be made routinely available.

DSAT will not publish any personal information, including photos, on its website without the permission of the individual.

When uploading information to any of the Trust websites, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

26. CCTV

CCTV is installed in various locations including schools to ensure safety. Use of CCTV is in adherence with the ICO's code of practice for the use of CCTV.

Whilst the Trust does not need to ask individuals' permission to use CCTV it is made clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about a school's CCTV systems should be directed to the school or workplace location. All CCTV footage will be kept in line with the **DSAT Document Retention Management Policy**.

27. Video and photography

Schools may take photographs and record images of individuals as part of normal activities.

Written consent will be obtained from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

The consent form will clearly explain how the photograph and/or video will be used.

Consent can be refused or withdrawn at any time.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

28. Data retention

Personal data that is no longer needed will be disposed of securely in line with the retention periods set out in the **DSAT Document Retention Management Policy**.

A third party may be commissioned to safely dispose of records on our behalf. The third party will be required to provide sufficient guarantees that it complies with data protection law.

29. Training

All staff and individuals involved in governance are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or processes make it necessary.

30. Policy review

This policy is reviewed every three years and will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

This policy was last reviewed in April 2020. The policy was approved Board of Trustees in May 2020.

Appendix 1: Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified. It includes: ▪ a person's name ▪ job title ▪ age ▪ postal or email address ▪ IP address, e.g. online identifier ▪ vehicle registration number ▪ bank details ▪ plus any other information that relates to them, e.g. a pseudonym.
Special category data	There are "Special Categories" of personal data and these include data revealing: ▪ race or ethnicity ▪ religious or philosophical beliefs ▪ trade union membership ▪ a person's health ▪ sex life or sexual orientation ▪ genetic or biometric data.
Processing	"Processing" relates to all actions or handling of personal data by manual or automated means, e.g. data collection, erasure and destruction plus everything in between including recording, use, disclosure, sharing and storage.
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed.
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Privacy notice	Sometimes referred to as 'fair processing notice' the privacy notice provides information to the data subject about data held about them. It also explains why the data is held, who it is shared with and for what purpose. It provides specific information about the data controller, the data protection officer and who to contact if they want more information.

Appendix 2: Legal framework

This strategy also takes into account legislation, including, but not limited to the following:

- General Data Protection Regulation 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This strategy will be implemented in conjunction with the following trust policies and procedures:

- Document Retention Management Policy
- ICT Acceptable Use Policy
- GDPR Data Subject Access Request Procedure (SAR)
- GDPR Data Subject Rights Requests Procedure
- Mobile Phone and Loaned Equipment Policy
- Data Security Incident Management Policy
- Freedom of Information Policy
- CCTV Policy
- School Workforce Privacy Notice
- Parent/carer Privacy Notice
- Pupil Privacy Notice
- Safeguarding & Child Protection policy