DATA PROTECTION POLICY

General Data Protection Regulations

Spring Term 2025

DUE FOR RENEWAL: Spring Term 2028

CHANGES

May 2018	Policy implemented
November 2020	Policy updated in line with Data Protection Officer guidance
October 2021	Policy reviewed and updated to reflect enhanced security measures in place when letters go home with pupils
March 2022	Policy reviewed, no changes made
June 2022	Policy reviewed and updated to reflect enhanced security measures in place when letters go home with pupils

March 2025

UK GDPR Compliance – Updated references from **EU GDPR** to **UK GDPR** and aligned legislation with **post-Brexit** requirements.

International Data Transfers – Clarified rules on **transfers outside the UK**, requiring **Standard Contractual Clauses (SCCs)** or **adequacy agreements**.

Personal Data Breach Reporting – Reinforced the **72-hour notification requirement** to the **ICO**.

Staff Training & Audits – **Mandatory annual GDPR training** for staff and **yearly audits by Plymouth City Council** to ensure compliance.

Data Retention & Security – Aligned retention policies with **ICO guidance** and emphasized **secure storage & disposal**.

UK Representative for Non-UK Entities – Added requirement for a **UK-based representative** if processing UK residents' data from abroad.

DPIA & Compliance Monitoring – Ensured **high-risk processing activities** undergo **Data Protection Impact Assessments (DPIA)**.

AI Procedures

CONTENTS

1. INTENTIONS

Discovery Multi Academy Trust supports the objectives of the Data Protection Act 2018 (DPA 2018) and intends to always conform to the requirements of the Act.

The DPA 2018 sets out six data protection principles that our Trust is responsible for and must be able to demonstrate compliance with. This policy details how the Trust will comply with these principles.

2. LEGISLATION AND GUIDANCE

The DPA 2018 makes provision for dealing with personal data. Most processing of personal data is subject to the General Data Protection Regulations (GDPR) which describes how personal information must be managed. The GDPR recognises changes in technology and the way organisations collect information. The DPA 2018 and the **UK GDPR** apply to all personal data regardless of the format. These frameworks, as enforced by the **ICO**, cover personal data processing within the UK.

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. The Information Commissioner's Office has responsibility for monitoring and enforcing the provisions of the GDPR and DPA 2018.

3. OUR TRUST'S ROLES AND RESPONSIBILITIES

This policy must be compiled fully by all Trustees, staff, volunteers, contractors and suppliers of Discovery Multi Academy Trust who collect, hold, process or deal with personal data for or on behalf of the Trust. **Staff who do not comply with this policy may face disciplinary action**.

3.1 The Board of Trustees

The Board of Trustees has overall responsibility for ensuring that Discovery Multi Academy Trust complies with all relevant data protection obligations.

3.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the Board their advice and recommendations on Trust data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Our DPO contact details are:

Liz Easterbrook
Data Protection Officer
Finance
Plymouth City Council
Ballard house
West Hoe Road
Plymouth
PL1 3BJ
Email: dataprotectionofficer@plymouth.gov.uk
Tel: 01752 398380

3.3 Chief Executive Officer

The Chief Executive Officer acts as the representative of the data controller on a day-to-day basis.

3.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy and any supporting policies and processes implemented by the Trust
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If there has been a definite or suspected data breach or if there has been a 'near miss'
    - If they are unsure whether or not they have a lawful basis to collect or process personal data for a particular reason
    - If they receive a data protection rights request from an individual
    - If they need to rely on or capture consent outside of the existing consent requirements of the Trust or if they need to draft a privacy notice
    - Transfer personal data outside the European Economic Area or use any third party that intends to do so
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

4. DEFINITIONS

Term	Definition
Data Subject	The identified or identifiable individual that the personal data being held or processed relates to.
Personal data	Any information relating to a natural identifiable person whether directly or indirectly.
Special category data	These are highly sensitive pieces of information about people. They are

	important because under GDPR they are afforded extra protection in terms of the reasons we need to have access and process that information. This is defined as data relating to: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Health – physical or mental • Sex life or sexual orientation • Data relating to criminal offences is also afforded similar special protection In education we also apply this special protection to other categories of personal data which is considered to be highly sensitive, such as: • Free Trust meals • Pupil premium eligibility • Special educational needs • Children in need/looked after children • Children Services interactions • Safeguarding
Processing	This includes anything that is done with personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, sharing, erasing or destroying. Processing can be automated or manual.
Data Controller	The organisation who (either alone or in common with other people or organisations) determine the purpose for which, and the manner in which data are processed.
Data Processor	A person or organisation who processes data on behalf of and orders of a controller.
Data audit/data asset register	The assessment of data and it's quality, for a

	specific purpose.
Lawful basis and conditions for processing	These are the specific reasons, set out in law, for which we can process personal data. There is one list for personal data (lawful basis article 6) and another list for processing special category data (article 9).
Data retention	How long we will hold information to carry out the processing job we need it for. At the end of a data retention period, personal data will be disposed of securely.
Subject Access Request (SAR)	This is where a data subject requests access to the information we hold about them.
Data Protection Impact Assessment (DPIA)	This is a process to consider the implication of a change we are introducing on the privacy of individuals' data, for example if we are introducing a new system.
Data breach	A personal data breach means the accidental or unlawful destruction, loss, alteration, disclosure or access to personal data. Breaches are either accidental or deliberate.
Automated decision making/profiling	This is when machines/software make decisions based on rules generated by the machine/software, without human intervention, about someone. Typically, it is the significance of the decision that drives the caution and concern here.

5. THE DATA CONTROLLER

Our Trust collects and processes personal data relating to parents, pupils, staff, those in a position of governance, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The Trusts registration number is **ZA240694**.

6. DATA PROTECTION PRINCIPLES

The data protection principles require that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay, (taking into account the purpose for which it is being processed)
- Kept in a form that aligns with UK GDPR, with appropriate safeguards for data stored beyond the UK
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

7. PROCESSING PERSONAL DATA

7.1 Lawfulness

We will only process personal data where we have grounds for that processing to take place. This is called a 'lawful basis' (legal reason) for processing and there are six options depending on our purpose and relationship with the individual. No single basis is 'better' or more important that the others and are highlighted below:

- **Consent:** the individual (or their parent/carer when appropriate – see section 9.2) has given clear consent for the Trust to process their personal data for a specific purpose
- **Contract:** the data needs to be processed so that the Trust can fulfil a contract we have with the individual, or the individual has asked the Trust to take specific steps before entering a contract
- **Legal obligation:** the data needs to be processed so that the Trust can comply with the law (not including contractual obligations)
- **Vital interests:** the data needs to be processed to protect someone's life
- **Public task:** 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 task or function has to have a clear basis in law
- **Legitimate interests:** 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)

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.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

7.2 Fairness and transparency

We will be clear, open and honest about the reasons we are collecting personal data and how we intend to use this. We will only process personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will produce Privacy Notices to inform individuals about the personal data we process, the reasons for this and who we may share this with. This will also inform them of their rights under the GDPR and DPA 2018.

7.3 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. The information we collect will be relevant and limited to what is necessary to fulfil the purpose for which it is being collected. We will be clear from the outset the reasons why we are collecting personal data and what we intend to do with it. This applies whether we collect the personal data directly from the individual or whether we collect their data from another source.

If we want to use personal data for reasons other than those specified when we first collected it, we will ensure that the new use is fair, lawful and transparent. We will inform the individuals concerned before we do so and seek consent where necessary.

We will take all reasonable steps to ensure that the personal data we hold is not incorrect or misleading and will keep this updated if this is necessary for the purpose we are using it. If we discover that personal data is incorrect or misleading we will take reasonable steps to correct or erase it as soon as possible.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for Trusts.

We will record our purposes for processing personal data in our data asset register and specify them in our privacy notice.

8. 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 will 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. 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 standalone 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.

Transfers to countries outside the UK must comply with **UK GDPR**. Data transfers to the EU are permitted under the adequacy decision, but transfers outside these areas require additional safeguards like **Standard Contractual Clauses (SCCs)**.

9.0 SUBJECT DATA RIGHTS OF INDIVIDUALS

9.1 Data protection rights of the individual

Individuals have certain rights under the DPA 2018 and the UK GDPR. These are detailed in the Trust's privacy notices. Individuals should contact the Trust's data protection officer if they would like to exercise any of their rights. If the Trust receives a request directly then they should contact the Data Protection Officer immediately. Please refer to the Trust's 'subject rights request policy' for full details of the access rights of the individual, how a request can be made and how we will respond to this.

9.2 Data protection rights of children

A child, (anyone under the age of 18) has the same data protection rights over their personal data as an adult. We will give personal data processed about our pupils' specific consideration as they may be less aware of the risks, consequences and safeguards concerned.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of processing their personal data. Therefore, the rights of most of our children, including giving consent, can be exercised by parents or carers of our pupils without the express permission of the pupil, provided we are satisfied that the request has come from a person with parental responsibility. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10. REQUESTS TO SEE THE EDUCATIONAL RECORD

There is no legal right for pupils or parents/carers to have access to their educational records. However if a child (or parent/carer of a child who cannot act for themselves or who has given consent) requests this we will consider granting access in line with the legal requirements of maintained Trusts. Please see the Trust's SAR policy to see how we will assess if a child has capacity to make such a request. The information included in the educational record will cover academic achievements, correspondence from teachers, local education authority, employees, educational psychologists etc. We will endeavour to provide this within 15 Trust days of receipt of a written request.

Requests should be made in writing to Alison Nettleship, Chief Executive Officer.

11. CCTV

We use CCTV in various locations around the Trust site to ensure it remains safe. We will follow the ICO's code of practice and their guidance for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it 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 the CCTV system should be directed to Alison Nettleship, Chief Executive Officer.

12. PHOTOGRAPHS AND VIDEOS

As part of our Trust activities, we may take photographs and record video images of individuals within our Trust.

We will obtain written consent from staff, parents/carers, or pupils (in line with section 9.2 of this policy – rights of children) for photographs and videos to be taken for communication, marketing and promotional materials. Any request for consent will clearly explain to staff, parent/carers or pupils what the photograph and/or video will be used for.

Consent can be refused or given for some or all of the purposes for which it is taken, for example:

- Within Trust on notice boards and in Trust magazines, brochures, newsletters, etc.
- Outside of Trust by external agencies such as the Trust photographer, newspapers, campaigns
- Online on our Trust website or social media pages

Consent can also be withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we may, with consent, include the child's first name, however, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Care will be taken to safeguard the device used to take photographs or video footage. Where possible the device will be encrypted and/or password protected and images/footage will be uploaded to the Trust's secure drive as soon as possible and then immediately deleted from the portable device. Images will not be stored to individual drives or to individual computer hard drives. Portable devices containing images not yet uploaded will be locked away when not in use.

See the Trust's 'Use of Photographic Images Policy' for more information on our use of photographs and videos.

13. DATA PROTECTION BY DESIGN AND DEFAULT

The GDPR has placed a legal requirement on us to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual's rights. We have practices in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointment of a suitably qualified Data Protection Officer;
- Data protection issues are considered as part of the design and implementation of systems, services and business practices;
- We will notify the DPO where the Trust's processing of personal data presents a high risk to the rights of individuals, and when introducing new technologies in order to complete a data protection impact assessments (DPIA);
- Data protection issues are considered for any activities by the Trust, both on and off site. We will anticipate the risks to data privacy and take steps to prevent loss;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;

- Only using IT systems, services and business practices where personal data is automatically protected. We will ensure that the same standards of data protection are applied;
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Training members of staff at induction and at regular intervals on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- Making records of our processing activities available to individuals so that they can determine how we are using their personal data. This includes:
    - The name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record (data asset register) of the type of data, how and why we are processing the data (including the lawful basis), how we control access and keep the data secure and retention periods.

14. DATA SECURITY AND STORAGE OF RECORDS

We will process personal data inline with ICO guidelines and protect it from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Our measures to achieve this include:

- Keeping paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data under lock and key when not in use;
- Not leaving papers containing confidential personal data on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Where personal information needs to be taken off site, staff must sign it in and out from the Trust office;
- Where personal information is taken off site, staff must take care to treat this information with care and keep it secure at all times, e.g. not leaving personal data in the boot of a car or on display where others may gain access to it;
- Any letters taken home by pupils containing personal information e.g. IEP's, SEN information, Parentpay letters, must:
    - Be checked by 2 members of staff including one teacher
    - The sender must make a note of how many pages are being printed to the document and add the number of pages to the front envelope
    - The checker must check the number of pages as well as adding their name, signature and the date checked and the envelope must be sealed
- Passwords that are at least 8 characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, pupils or governors should not store personal data on their own personal devices.
- In exceptional circumstances and only where permission has been granted, if staff or governors do store personal data on their personal devices they are expected to follow the same security procedures as for Trust-owned equipment - see our acceptable use agreement;
- Where we need to share personal data with a third party, we carry out due diligence, put in place a data sharing agreement and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).
- We will not keep data for longer than we need it. Data will be retained in line with the Information and Records Management Society's toolkit for Trusts.
- We will periodically review the data that we hold and securely dispose of or anonymise it when it is no longer needed.
- Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
- We will shred or incinerate paper-based records, and overwrite or delete electronic files. Hard drives will be wiped before physical destruction when they have reached the end of their life. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. PERSONAL DATA BREACHES

We will notify the **ICO** of any personal data breaches that pose a risk to the rights and freedoms of individuals, in accordance with **UK GDPR**. This must be done within **72 hours** of becoming aware of the breach.

16. MONITORING ARRANGEMENTS

This policy will be reviewed and updated if necessary **every 2 years** and shared with the full Board of Trustees.

17. APPOINTMENT OF A UK REPRESENTATIVE

Data will be retained in line with the **ICO's updated guidelines** and the **Information and Records Management Society's toolkit for Trusts**, ensuring compliance with UK-specific data retention laws

18. STAFF TRAINING AND GDPR AUDIT

To ensure continued compliance with UK GDPR and data protection laws:

All staff will receive mandatory annual GDPR training, covering key updates, data security, and individual responsibilities. This will include any changes in UK GDPR or relevant legislation.

The Trust will conduct an annual GDPR audit, facilitated by **Plymouth City Council**. This audit will review data protection practices, assess compliance with the UK GDPR, and recommend any necessary improvements

19. Artificial Intelligence (AI) and GDPR Compliance

The Trust acknowledges the increasing use of Artificial Intelligence (AI) in data processing and ensures compliance with **UK GDPR** by adhering to the following principles:

- **Lawful Basis for Processing**: AI systems must have a **clear legal basis** for processing personal data, ensuring transparency and fairness.
- **Automated Decision-Making**: Decisions solely made by AI that significantly impact individuals require **human oversight** and must allow for appeals.
- **Data Minimisation**: AI models should only process **necessary** personal data to achieve their intended purpose.
- **Bias & Accountability**: AI systems must be regularly **audited** to detect **bias** and ensure compliance with **data protection impact assessments (DPIAs)**.
- **Security & Risk Mitigation**: AI-driven data processing must comply with **strict security protocols** to prevent unauthorised access or misuse.

The Trust will **regularly review AI usage** and ensure compliance with evolving **ICO guidelines** on AI and data protection.