Data Protection Policy

Document control			POLICY LEVEL: Trust / Statutory	
Approved by	Trust Board		**Approved Date**	17 March 2022
Published Location	www.dartmoormat.org		**Next Review**	01 March 2025
Version	***Date issued***	***Author***	***Update information***	
V1.0	23 May 2018	DPO	First published	
V1.1	24 May 2018	DPO	Appendix 1 deleted	
V1.2	18 July 2018	DPO	Review date updated	
V1.3	02 March 2022	J Coundon	Complete revision	

Introduction

Our Data Protection (DP) Policy lays out our approach to data protection. We recognise the importance of protecting the personal data we are entrusted with, and this policy sets out how we comply with relevant legislation.

If you have any queries about this Policy, please contact our Data Protection Officer, whose details can be found in our Privacy Notices.

Scope and Responsibilities

This Policy applies to all staff, including temporary staff, consultants, governors, volunteers, and contractors, and anyone else working on our behalf.

All staff are responsible for reading and understanding this policy before carrying out tasks that involve handling personal data, and for following this policy, including reporting any suspected breaches of it to our Data Protection Officer.

All leaders are responsible for ensuring their team read and understand this policy before carrying out

Tasks that involve handling personal data, and that they follow this policy, including reporting any suspected breaches of it.

Our Data Protection Officer is responsible for advising us about our data protection obligations, dealing with breaches of this policy, including suspected breaches, identified risks, and monitoring compliance with this policy.

Data Protection Legislation & Regulator

Relevant legislation includes:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for
- Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing ("marketing" includes fundraising and promoting an organisation's aims, not just selling.)
- Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.

Data Protection Policy

In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.

Breaches of data protection legislation can result in significant monetary penalties and damage to reputation, as well as the risk of real harm to people whose data is handled in an unfair or unlawful way. Individual members of staff may be prosecuted for committing offences under Sections 170 – 173 of the DPA 2018.

Our Data Protection Objectives

We are committed to making sure that:

- Personal data is only processed in keeping with legal data protection principles. The principles include data being processed lawfully, fairly and in a transparent manner; data being processed only for specific, explicit and legitimate purposes; data being adequate, relevant and accurate, data not being kept longer than is necessary; and data being kept secure
- We adopt a "Privacy by Design" and "Privacy by Default" approach
- We can demonstrate our accountability and compliance
- The people whose data we hold (Data Subjects) understand the ways and reasons why we process their data, and can easily and fairly exercise their rights around their data
- We only share personal data when it is fair and lawful to do so, and when we share data, we do it in a safe and secure way
- Data is not transferred outside of the European Economic Area (EEA) except where the EU has made an 'adequacy decision' or the transfer is covered by 'appropriate safeguards', as defined in GDPR Article 46, or there is a derogation, or a specific situation as defined by GDPR Article 49
- All data breaches, including near misses, are managed properly, and reported appropriately, so we can minimise any risks and improve practices in the future. This includes any breaches of the Data Protection Act (DPA 2018) where the individual responsible may be liable.

Our Data Protection Rules

We follow the legal Data Protection Principles:

i. **Fair, lawful and transparent processing**: The reason for processing of personal data must meet one of the legal conditions listed in Article 6 of the GDPR, and when "special categories" of personal data are being processed, the purpose must also meet one of the legal conditions listed in Article 9 of the GDPR. "Special categories" are information about a person's race or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, genetic and biometric data, sexual life, or sexual orientation.

Legal conditions: See Annexe 1 for an explanation of the Legal Conditions for Processing.

Data Protection Policy

Other legislation: All processing must also comply with the other data protection principles and any other relevant legislation, including the DPA 2018 and the Privacy and Electronic Communications Regulations (PECR) as appropriate. Any individual who obtains, discloses, or retains data when they do not have permission to do so may be committing an offence under the DPA 2018 Section 170. All electronic "direct marketing" is subject to the PECR, which require us to obtain consent before sending direct marketing messages electronically.

Transparency: To be fair and transparent, our data processing, including how and why we process data, is explained in our Privacy Notices. We also explain how and why data will be processed at the point where we collect that data, as much as is reasonably possible, and especially if the processing is likely to be unexpected.

ii. **Purpose limitations**: We only use the data we collect for the reasons we explained in our privacy notice. If we need to use it for another reason, we will inform our data subjects of the new reason for processing before we do it.

iii. **Data limitations**: We minimise the amount of data that we collect and process, keeping it to only what is necessary for the reasons we are collecting it. We should never collect or keep any personal data "just in case".

iv. **Data accuracy**: We will always try to make sure the data we collect and hold is accurate and keep it up to date as appropriate.

v. **Data retention**: We will only keep personal data for as long as is necessary for the reasons for which we are processing it, and we will be transparent with our data retention schedules. Any individual who purposefully retains data that they do not have permission to be holding, may be committing an offence under the DPA 2018 Section 170.

vi. **Data security & integrity**: We use both technical and organisational security measures to protect data from unauthorised or unlawful processing, or from accidental loss, destruction, or damage. Security measures should be appropriate to the level of risk involved in the data and the processing. Our measures include but are not limited to: technical measures such as IT systems security, IT access controls, pseudonymisation, and encryption; and organisational measures such as business continuity plans, physical security of our premises and data, policies, procedures, training, audits and reviews.

Security should be considered at all times. This includes when data is being stored, used, transferred, or disposed of, whether the data is electronic or hard copy, and regardless of how and where the data is being accessed and stored, especially when data is sent or taken off site, or to another organisation.

Any individual who purposefully re-identifies pseudonymised information without permission may be committing an offence under the DPA 2018 Section 171.

Privacy by Design & Default

Wherever possible, we adopt a Privacy by Design & Default approach. When we are planning projects or new ways of working that involve processing of personal data, we will consider the data protection implications, and how to make sure we meet legal and good practice requirements, from the planning stages, and keep a record of the outcomes.

For particularly high-risk processing, whether from a new or adapted way of working with personal data, we will do this using Data Protection Impact Assessments (DPIAs), to document the risks, decision-making process and decisions made, including recommendations and actions.

High risk processing includes processing the data of children as children are vulnerable data subjects and the data processed is often sensitive or highly personal data.

A DPIA may be carried out to decide if any changes or new controls are needed for existing ways of working.

To demonstrate and support our compliance with data protection legislation, we keep records of the processing we carry out, we have appropriate policies and procedures in place, we train our staff in data protection, we have a Data Protection Officer in post, we carry out regular audits and reviews of our activities, and we record and investigate data security breaches.

Our records of processing include our contact details and information about why we are processing personal data, what types data we process, the categories of people we process data about, information about how long we hold the data for, and general information about our security measures, as well as the types of external the data is shared with, including any transfers outside of the EEA, and the safeguards in place if data is transferred outside the EEA.

Rights

We process personal data in line with the legal rights of data subjects', including their right to:

- Be informed about their data being processed, which links to the first DP Principle of fair, lawful and transparent processing
- Request access to their data that we hold (sometimes requests are known as [Data] Subject Access Requests, or DSARs or SARs)
- Ask for inaccurate data to be rectified
- Ask for data to be erased (sometimes known as the "right to be forgotten"), in limited circumstances
- Restrict processing of their data, in limited circumstances
- Object to the processing, in some circumstances, including stopping their data being used for direct marketing
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person
- Not be subject to automated decision making or profiling, if it has legal effects or similarly significant effects on the data subjects
- Withdraw consent when we are relying on consent to process their data
- Make a complaint to the ICO or seek to enforce their rights through the courts.

We will respond to, and fulfil, all valid requests within one calendar month, unless it is necessary to extend the timescale, by up to two months in certain circumstances. Not all the rights are absolute rights, and we cannot always carry out the requested action in full, or at all. For example, the right to erasure may be limited in some

circumstances because we are required to keep some records, and a number of exemptions in the DPA 2018 apply to SARs, meaning we can withhold some information in some situations.

In responding to requests, we also explain to data subjects they have the right to make a complaint to the ICO or seek to enforce their rights through the courts.

Any individual who purposefully alters, defaces, blocks, erases, destroys, or conceals information to prevent it being provided to a data subject who has requested it, and has a right to receive it, may be committing an offence under the DPA 2018 Section 173.

Data Sharing

Data Processors

We rely on the services of a number of external parties to support our work (both management and curriculum). These may include people, companies, systems, and software that process personal data as part of the work they do on our behalf. These are our "data processors". When working with data processors, we will carry out appropriate due diligence checks to make sure that they can provide sufficient guarantees that they will comply with data protection legislation, including keeping data secure and cooperating with us to uphold data subjects' rights. We will require contractors and their staff to comply with this DP Policy.

In accordance with GDPR Article 28, we will appoint data processors only on the basis of a legally binding, written contract, that requires them to, amongst other things: only process personal data based on our instructions; keep the data secure; assist us to comply with our legal obligations and uphold data subjects' rights; delete or return the data at the end of the contract; and allow inspections and audits of their processing activities. Data Processor contracts, and compliance, will continue to be monitored throughout the contract period.

Third Parties

We will only share personal data with any other external, including other data controllers such as agencies and organisations, when the sharing meets one or more appropriate legal condition, and is carried out in keeping with the data protection principles and while upholding the rights of data subjects. Where necessary we will enter into Data Sharing Agreements (DSA), or similar agreements, to help facilitate the sharing of personal data. A DSA does not make the sharing lawful, it only provides a framework to work within, to help share data in an effective and safe way that respects people's data protection rights, when an appropriate and lawful reason to share the data has been identified.

Non-EEA data transfers

Personal data will not be transferred outside the EEA unless it is allowed by the conditions in Chapter V of the GDPR. This includes storage of data on cloud-based servers that are located outside the EEA.

Data Protection Policy

Data Protection Breaches

All breaches, or suspected breaches, of this policy will be reported immediately to the Data Protection Officer, and will be investigated appropriately, corrective, and preventive action taken and recorded. This includes, but is not limited to, any personal data we handle being lost, or being shared, destroyed, changed or put beyond use when it should not be.

Specifically, breaches that are likely to result in a risk to the rights and freedoms of data subjects, will be reported to the ICO within 72 hours of the school becoming aware of the breach.

If a breach is likely to cause a high risk to affected data subjects, we will also tell the data subjects, as soon as possible and without undue delay, to allow them to take any actions that might help to protect them and their data. We will also consider informing data subjects about a breach, even if there is not a likely high risk, if it is an appropriate step for other reasons, such as preserving open communication.

We will log all breaches, including those that are not reportable to the ICO.

Data Protection Policy

Annexe.1 Legal Conditions for Processing

Introduction

"Personal data" means any information where a living person is either identified or identifiable, from the information alone, or with other information. Personal data can include written information, pupil work, photographs, CCTV and film footage or voice recordings, in electronic format (which can include in social media, apps, databases or other electronic formats) or hard copy (including copies printed from electronic sources, and handwritten data when it is part of a filing system or intended to be filed).

"Special category data" is personal data that needs more protection because it is sensitive.

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data (where used for identification purposes)
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation
- In addition, the DfE advises that Pupil Premium/FSM status is treated as Sensitive Data.

"Data Subjects" include our pupils, staff, contractors, parents, local authority contacts, and anyone else we might come into contact with.

"Data Controller" means the school, alone or jointly with other Data Controllers, decides on why and how personal data is processed.

"Processing" means collecting, storing, using, sharing and disposing of data.

"Processors" are the external bodies who processes personal data on behalf of the controller.

Our Role and Bases for Processing

The role of any school is to educate and safeguard children. These are statutory obligations and come from various Acts and statutory instruments that can be found here.

This means the overwhelming volume of our collection and processing data is covered under Article 6 (1) c of the General Data Protection Regulations 2018: processing is necessary for compliance with a legal obligation to which the controller is subject:

- Equality Act 2010
- Education (Governors' Annual Reports) (England)(Amendment)Regulations 2002.
- Special Educational Needs and Disability Act2001
- Health & Safety of Pupils on Educational Visits 1998

Data Protection Policy

- Safeguarding Vulnerable Groups Act 2006
- Disability Discrimination Act(s)
- The Education Act 1944, 1996, 2002, 2011
- The Education & Adoption Act 2016
- The Education (Information About Individual Pupils) (England) Regulations 2013
- The Education and Skills Act 2008
- The Education (Pupil Registration) (England) Regulations 2006
- Statutory Guidance for Local Authorities in England to Identify Children Not Receiving Education – February 2007)
- The Education and Inspections Act 2006
- The Children Act 1989, 2004
- The Childcare Act 2006
- The Children & Families Act 2014
- Local Safeguarding Children Boards Regulations 2006 (SI 2006/90)
- The Localism Act 2011 Contract (traded services)

Some of our functions in educating and safeguarding children that cannot be directly linked to a statutory function above may be carried out under Article 6 (1) e of the General Data Protection Regulations 2018: processing is necessary for the performance of a task carried out in the public interest.

Where we process special category data, we do so under the General Data Protection Regulation Article 9 and the Data Protection Act 2018 Schedule 1 Part 1 and Part 2. We have a separate Special Category Data Policy document which sets out in detail what lawful basis we rely on for processing Special Category Data as is required by the Data Protection Act 2018 Schedule 1 Part 4.

When we wish to process data for any other reason, we will ask for consent as per Article 6 (1) a of the General Data Protection Regulations 2018. Typically, this will be for areas of our work that includes the public celebration of our school and pupils' work. Data Subjects retain the right to change their consent preferences at any time by notifying the school office.

Data Subjects' Rights

All of our data subjects have a number of rights – these are detailed above.

To exercise these rights or for further help and information about processing and our commitment to keeping data safe, please contact our Data Protection Officer:

Data Protection Officer	Education Data Hub
DPO Email:	dpo@dmatschools.org.uk
DPO Phone:	01629 532888
DPO Address:	Room 396, North Block, County Hall, Smedley Street, Matlock, Derbyshire, DE4 3AG