Drapers' Multi-Academy Trust

Data Protection Policy

Version 2

Data Protection Policy
Drapers' Multi Academy Trust
September 2018
Review date: September 2020
Policy Holder: Steve Glazebrook

1. Context and overview

1.1 The Drapers' Multi Academy Trust [the MAT] needs to gather and use certain personal information about individuals. This can include learners, parents/carers, staff, MAT Directors, Governors of Local Governing Bodies and volunteers.

1.2 All data must be collected, stored and managed in accordance with UK and EU law, and in line with the MAT's ethos and values. Individuals retain the rights over their own data at all times. The Mat's use of their data must be fair and lawful, and the MAT must be open and honest about what it does with people's data.

1.3 All data is processed is in accordance with the rules as laid down in statute, including the General Data Protection Regulations, the Education Act 1986, the Education (Pupil Information) (England) Regulations 2005, the Education and Skills Act 2008, the Apprenticeship, Skills, Children and Learning Act 2009, and the expected provisions of the Data Protection Act 2018.

1.4 This Policy has been framed in accordance with the guidance on best practice from the Department for Education (DfE).

2. Key principles

- Individuals retain rights over their data
- Data should be collected fairly and lawfully and used only in ways that the individual would expect
- Data should only be kept for as long as is necessary
- Data integrity and security is paramount
- Data governance is actively managed at all levels of the organisation, to minimise risks to both the individual and the organisation
- All collection and use of data is open and honest

3. Why this policy exists

3.1 This policy ensures that the MAT respects the rights of all individuals whose data it collects, including learners, parents/carers, staff, MAT Directors, Governors of Local Governing Bodies and volunteers. It encompasses legal responsibilities and best practice. By being open and honest with individuals the MAT can demonstrate that people can have confidence that the MAT can handle personal data with integrity. Routine application of these principles will also help protect the MAT from the risk of data breaches and unauthorised access to personal information.

4. Data Protection Law and Principles

4.1 The use of personal data is governed by EU and UK law. This is enhanced and explained by case law and best practice.

4.2 In order to comply with the law, personal data must be collected fairly and lawfully. It must be stored safely and managed securely. It must not be disclosed to anyone who does not have authority to see it.

4.3 The General Data Protection Regulations (GDPR) sets out how data should be obtained, stored and handled. These regulations underpin lawful use of data. These provide the foundation for good data governance. These principles are enhanced by a range of powers for individuals to control how their data is processed and stored:

5. Policy Scope

5.1 This policy applies to:

- All schools within the Drapers' Multi Academy Trust (the MAT)
- All Teaching staff, support staff, Directors of the MAT, Governors of the Local Governing Bodies and volunteers
- Contractors, suppliers and anyone working on our behalf

6. Responsibilities under this policy

6.1 Everyone who works with or for the MAT has some responsibility for ensuring that data is handled safely, securely and appropriately.

6.2 There are key roles within the organisation that carry specific responsibilities.

6.3 The Board of Directors is the strategic body for the MAT. They bear ultimate responsibility for ensuring that all our legal obligations are met. They are accountable for any failure to abide by the correct regulations and for any impact that they may have on our learning community and our reputation within the local area.

6.4 The Principal and the Senior Leadership Team are the operational leads for each school within the MAT. They must ensure that all relevant policies and procedures are in place, and that practice follows the policy in each school. They must liaise with the Data Protection Officer in the event of any data governance issues that require attention, and have overall responsibility for setting an appropriate tone and culture of respect for personal data within the school.

6.5 The Data Protection Officer (DPO) plays a key in providing expert advice and guidance to the MAT Board, the Local Governing Bodies and the Senior Leadership Team in each school. It is the DPO's responsibility to update senior management and the MAT Board about Data Protection issues, and to update policies and procedures in accordance with an agreed schedule and following legislative and best practice updates. The DPO is responsible for overseeing training and guidance for all staff, and for liaising with third party suppliers, contractors and partners if they handle personal

data. The DPO is also responsible for overseeing any Subject Access Requests, and for handling the response to any data breaches, including being the point of contact for the public and notifying the ICO as necessary.

6.6 The IT Manager is responsible for ensuring the physical and virtual integrity of IT data storage services, systems and equipment. Ensuring all IT security meets acceptable professional standards appropriate to the needs of the organisation and that access to all electronic systems, databases or files is managed in accordance with the relevant polices. The IT Manager is also responsible for liaising with any third party used for processing data, such as an HR / payroll supplier or cloud computing provider, to ensure appropriate levels of protection for all personal data. The IT Manager has responsibility for making sure that customer-facing applications such as websites or online forms comply with relevant regulations including cookie policies and privacy notices. The IT Manager oversees the life-cycle of data, software and hardware, ensuring that the processes for deleting or encrypting files are in accordance with the appropriate retention policy function.

7. What is personal data?

7.1 Personal data is information about a person - anything that would allow someone to identify a living individual. Processing that data means obtaining, using, and transferring data, and storing it in any system that allows it to be found again, such as a computer database or filing system.

8. Our Privacy Notice

8.1 The MAT has taken all reasonable steps to ensure that individuals are aware their data is being processed. Individuals are advised what is being used, how it is being used, how long it will be kept for, and how they can exercise their rights in respect of that data.

8.2 The MAT's Privacy Notice sets out how data is collected, what data is collected, the lawful basis for that, and how long we it is retained. It includes information on with whom data is shared and the lawful basis for such sharing. It also sets out how people can request copies of data held about them. The Privacy Notice is included in any marketing or information literature the MAT produces. The Privacy notice is also available on request, and is on the MAT's website.

9. Keeping personal data secure

9.1 Once personal data has been lawfully and fairly collected and processed, it must be safely stored, kept up to date, and safely accessed. Storing data in a way that complies with the regulations is a mix of common sense, clear processes and application of strong IT solutions.

9.2 The only people with access to personal data at the MAT are those who need it for their work. The IT systems and file storage have granular levels of permission, to ensure that people only see personal data if required for operational reasons and for the benefit of teaching and learning.

9.3 Strong passwords are used to access electronic resources and IT systems. These should never be shared with other people, or written down. The MAT sets an appropriate password policy and requires passwords to be changed on a regular basis.

9.4 Personal data must only be disclosed to those who are authorised to see it, both within and outside the organisation. If there is any doubt about the identity of the person requesting access to information, or doubt as to whether they should be allowed to see it, then information will not be disclosed.

9.5 Data is only shared with those people who are authorised to see it. This is in accordance with the MAT's legal obligations and with the lawful and legitimate requirements of the MAT. The MAT's Privacy Notice explains with whom data may be shared, the lawful basis for any sharing, and the circumstances in which individuals can object to data being shared.

9.6 The MAT will ensure that training is made available to all staff.

10. Data use and transfer

10.1 Data must only be used for the purpose it was first obtained. Personal data should not be shared informally, either internally within the MAT or any external organisation.

10.2 Staff should follow simple checks when transferring data outside the organisation via post or email, to ensure that personal data goes to the correct recipient. The MAT uses a simple checklist when sending personal data by post, to add an extra layer of security and checking to its data transfers.

10.3 Extra care must be taken when sharing data via email. This might include encryption or use of a secure email client, but this will depend on the type of information being shared and the recipient.

10.4 Data should not be stored on personal IT devices. In particular staff must not email school documents to their personal email addresses or use personal email accounts for work purposes. If data needs to be transferred outside of the secure school network, staff should use their secure school email account for doing so.

11. Marketing and Promotion

11.1 The MAT does carry out marketing and promotion.

11.2 When requesting school visits or brochures, or signing up for more information at Open Days, The MAT advises all prospective parents about how their data will be stored, how often they may be contacted, and gives them the opportunity to decline to be contacted in the future.

11.3 The MAT ensures that anyone receiving marketing or promotion communications has given positive consent to receiving those communications, in the format that they are sent out.

11.4 All marketing and promotion communications include a simple process for addressees to apply to be removed from future communications.

12. CCTV across the MAT

12.1 The MAT does use CCTV cameras across schools within the MAT. This is to ensure the safety and security of those in its learning community, and to protect the school sites from damage. The use of CCTV follows best practice guidelines as laid down by the ICO.

12.2 Images recorded by the CCTV cameras are stored on a separate server, in a secure location. They are retained for a maximum of 21 days, after which time they are securely overwritten.

12.3 Access to the images is restricted to specified people within the MAT. CCTV footage is only viewed in response to an incident or an allegation being made.

12.4 In some circumstances the images on the CCTV system are of a sufficient quality to allow the identification of the faces of individuals. Copies of the relevant parts of the CCTV footage may be stored securely in order to assist and support investigations into incidents or allegations being made.

12.5 In certain circumstances CCTV footage may be shared with partners or other agencies. This may include members of MAT Directors, Senior Leadership Teams, members of Local Governing Bodies, parents, the Local Authority and the Police.

13. Getting your consent to process your personal data

13.1 There may be times when the MAT would wish to process data in a way that requires consent. This could include taking photographs or images of individuals engaging in school activities, or adding contact details to any marketing or promotional mailing lists. It would also include getting agreement to take and use finger or

thumbprint map information, to be used to access cashless/online catering payment services.

13.2 The MAT ensures that consent is obtained in a positive and clear way. Consent, may be refused and such refusal will not impact on the individual's ability to join in the full-range of activities and opportunities across the MAT. If an individual does not wish to use thumb or fingerprint recognition, then an easy alternative will be provided. The MAT ensures that consent may be quickly and easily withdrawn, should an individual changes their mind about the MAT processing their data in these ways.

14. Subject Access Requests

14.1 Individuals have the right to ask to see a copy of any information held about them by the MAT. This is known as a Subject Access Request (SAR).

14.2 SAR's can be made by contacting: admin@drapers-schools.com

15. Breaches of this policy

15.1 If the MAT considers that this policy has not been followed in respect of personal data, then any breach will be managed in accordance with the MAT's Disciplinary Policy.