Academies Trust

8th Floor, Angel Square,
Manchester, M60 0AG

Data Protection Policy

Approved by the Trust Board on 3 October 2024

Applicable from 4 October 2024

This document will be reviewed annually, or more frequently when significant changes are made to the law.

Contents

1. Introducing our DP Policy

1.1. 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.

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

2. Scope and Responsibilities

2.1. This Policy applies to all staff, including temporary staff, consultants, members, trustees, community council members, volunteers, and contractors, and anyone else working on our behalf.

2.2. 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 Head of Data Protection.

2.3. All leaders are responsible for ensuring that 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.

2.4. Our Head of Data Protection 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.

3. DP Legislation & Regulator

3.1. Relevant legislation includes:

3.1.1. UK General Data Protection Regulation (UK GDPR);
3.1.2. 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;
3.1.3. Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing ("marketing" includes fundraising and promoting an organisation's aims, not just selling.)
3.1.4. Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.
3.1.5. Human Rights Act 1998
3.1.6. Computer Misuse Act 1990, which covers unauthorised access to, and use of, computers and computer materials.

3.1.7. Education (Pupil Information) Regulations 2005 which gives parents the right to access their child's education record (applicable to our special schools only)

3.1.8. Protection of Freedoms Act 2012

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

3.3. 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.

3.4. Individual members of staff may be prosecuted for committing offences under Sections 170 – 173 of the DPA 2018.

4. Our DP Objectives

We are committed to making sure that:

4.1. 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 valid purposes; data being adequate, relevant and accurate; data not being kept longer than is necessary; and data being kept secure;

4.2. We adopt a "Privacy by Design" and "Privacy by Default" approach;

4.3. We can demonstrate our accountability and compliance;

4.4. 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;

4.5. 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;

4.6. Data is not transferred outside of the UK except where the country has an 'adequacy decision' or the transfer is covered by 'appropriate safeguards', as defined in UK GDPR Article 46, or there is a specific situation that allows the transfer as defined by UK GDPR Article 49;

4.7. 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.

5. Our DP Rules

5.1. 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 UK GDPR. In addition, 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 UK 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, sexual life or sexual orientation, or genetic and biometric data.

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

Other legislation: All processing must also comply with the other DP 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 requires us to obtain consent before sending direct marketing messages electronically by email or SMS ("marketing" includes fundraising and similar types of messages, not just selling.)

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 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 schedule which can be found on the Trust website. Any individual who purposefully retains data that they do not have authority for 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 ICT systems security, ICT 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 is 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.

Organisational measures include staff training. All staff receive role-based training on appointment, and then every 2 years.

Specific areas of compliance are addressed in a bitesize suite of short courses, accessed regularly by relevant staff.

5.2. Privacy by Design & Default

5.2.1. 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.

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

5.2.3. High risk processing includes processing the data of children, especially if processing special categories of data about children.

5.2.4. A DPIA is always required before setting up CCTV or biometric systems, or similar tracking technologies.

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

5.3. 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 (this statutory role is part of the remit of our Head of Data Protection), we carry out regular audits and reviews of our activities, and we record and investigate data security breaches.

5.4. 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 organisations the data is shared with, including any transfers outside of the UK, and the safeguards in place if data is transferred outside the UK.

6. Rights

6.1. 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 a Subject Access Requests, 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 data-related rights through the courts.

6.2. 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.

6.3. 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 in a SAR 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.

7. Data sharing

7.1. Data Processors

7.1.1. We rely on the services of a number of external organisations to support our work (both management and curriculum). These 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".

7.1.2. When working with data processors, we 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.

7.1.3. In accordance with UK 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.

7.1.4. Data Processor contracts, and compliance, will continue to be monitored throughout the contract period.

7.2. Third Parties

7.2.1. We will only share personal data with any other external organisation, including other data controllers such as agencies and other schools, when the sharing meets one or more appropriate legal conditions, and is carried out in keeping with the data protection principles and while upholding the rights of data subjects.

7.2.2. Where necessary we will enter into Data Sharing Agreements (DSA), or similar agreements, to help facilitate the sharing of personal data.

7.2.3. 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.

8. Non-UK data transfers

8.1. Personal data will not be transferred outside the UK unless it is allowed by the conditions in Chapter V of the UK GDPR, including having appropriate safeguards in place or the transfer being necessary for a specific situation that allows it. A "non-UK transfer" includes storing data on cloud-based software and systems where the servers that are located outside the UK, or where data remains in the UK, but is under the control of a non-UK service provider.

9. Data protection breaches

9.1. All breaches, or suspected breaches, of this policy will be reported immediately to the Head of Data Protection, 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. This also includes Cyber Incidents/Attacks.

9.2. Specifically, breaches that are likely to result in a risk to any rights and freedoms of the data subjects affected, will be reported to the ICO within 72 hours of the relevant academy or central team becoming aware of the breach.

9.3. 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 we are not legally obliged to, if it is appropriate for other reasons, such as preserving open communication.

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

10. Artificial Intelligence (AI)

10.1. We recognise that technology is rapidly evolving and are committed to remaining at the forefront of developments, adapting our ways of working as necessary.

10.2. AI is an integral part of the modern world and whilst this offers numerous opportunities for enhancing teaching, learning, and administrative processes, there are also potential risks, including to data protection principles, that must be explored.

10.3. In order to foster a responsible environment for the use of AI in education, upholding privacy, fairness, and transparency for the benefit of all involved, AI must not be used without prior authorisation from a member of the Trust Senior Leadership Team, and completion of a full data protection impact assessment.