Data Protection Policy

Last review date:		June 2024	
Next Review date:		June 2025	
Statutory Policy:		Yes	
Date	**Version**	**Reason for change**	**Source**
June 22	V2.0	Updates	Data Protection Officer
June 23	V2.1	2. Insert reference to records management guidance 3. Update to legislation references 4.6 Insert duty to inform DPO of new data sharing arrangements 6. Insert additional security measures 7. changes to process for data sharing 11. Insert duty to notify DPO of information rights requests	Data Protection Officer
June 24	V2.2	2. Insert ICO registration number 4.6 Insert addition requirements for staff in relation to data security, privacy and confidentiality 6. Insert DPO compliance checks Insert reference to DPIA requirements Insert reference to AI risk checks 9. Clarify responsibility for the use of images taken by parents/visitors 11.8 Insert reference to AI to automated decision making and profiling	Data Protection Officer

1. Aims

Matrix Academy Trust (MAT) is committed to upholding the key principles within data protection law.

This policy sets out how we will do that, by:

- applying data protection law to the day-to-day work of the Trust and its Academies;
- clarifying roles and responsibilities with respect to our data protection duties;
- outlining the ways we will process different kinds of personal data, including the various security arrangements we will put in place; and
- explaining how we will uphold the rights people have under data protection law.

2. About this policy

This policy applies to all personal data used by the Trust, or any of its Academies, the Teaching School and the SCITT to carry out its functions. It does not form part of any contract of employment and may be amended at any time.

Any breach of this policy – by any staff member, apprentice, volunteer, governor or Trustee, of the Trust and/or any of its Academies – may result in disciplinary or other action.

This policy meets the requirements of the UK GDPR and Data Protection Act 2018. It is based upon guidance from the Information Commissioner's Office (ICO).

It also meets the requirements of the Protection of Freedoms Act 2012.

This policy links with our:

- Privacy Notices;
- Retention Schedule and Records Management Guidance;
- Freedom of Information Policy
- Data Protection Guidance for staff and volunteers;
- ICT acceptable use Policy; and
- CCTV Procedures.

Matrix Academy Trust is a data controller registered with the Information Commissioner's Office (registration number: ZA185164)

3. Definitions

In this policy, the functions of the Trust and/or its Academies are the provision of education as well as any pastoral, business, administrative, community or similar activities associated with that provision. References to our functions are references to these activities.

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. Examples include: contact details; identification numbers; assessment data; location data; online identifiers; and so on.
Special category data	Types of personal data that are more sensitive, and so need more protection. It includes information about and individual's: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetics; • biometrics, where used for identification purposes; • physical or mental health; and • sex life or sexual orientation.
Criminal offence data	Any personal data relating to the commission of, or proceedings for, any criminal offence committed or alleged to have been committed by a person.
Processing	Anything done to personal data, including: collecting; recording; organising; structuring; storing; adapting; altering; retrieving; using; disseminating; erasing; or destroying. Processing can be manual or automated.
Data protection law	All laws applicable to England and Wales that relate to the processing of personal data – as may be amended, re-enacted, replaced or superseded from time to time – including: • the General Data Protection Regulation (UKGDPR) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426); and • the Data Protection Act 2018.
Data subject	The identified, or identifiable, living individual whose personal data is processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data. Matrix Academy Trust is the data controller for all personal data, including that which is processed by its Academies, used to carry out its functions.
Data processor	A person or organisation, other than an employee of the Trust or any of its Academies, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security, or action leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Roles and responsibilities

4.1 Board of Trustees/Directors

The Trust Board has overall responsibility for ensuring that MAT complies with all relevant data protection obligations to which it is subject. This duty may be delegated to the Trust's Audit and Risk Committee.

4.2 Parent Advisory Forum

Parent Advisory Forum may scrutinise their Academy's compliance with this policy and with data protection law more broadly.

4.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for:

- overseeing the implementation of this policy;
- monitoring the Trust's overall compliance with this policy and data protection law;
- advising on the development of related policies, procedures and guidelines;
- supporting with Data Protection Impact Assessments;
- acting as a contact point for data subjects and the supervisory authority; and
- advising and supporting the Academies to meet their data protection obligations
- reporting on their activities, including any advice and recommendations about any data protection issues, directly to the Board of Trustees, or a relevant Committee;
- investigating personal data breaches;
- responding to information requests.

Our DPO support is provided Services 4 Schools Ltd, they can be contacted by email at: dpo@matrixacademytrust.co.uk

4.4 Data Protection Leads

Data Protection Leads are responsible for:

- Liaising with the DPO to advise and supporting the Academies to meet their data protection obligations;
- developing and maintaining any procedures and associated documentation required to operationalise this policy;
- ensuring a consistent approach to data protection across the Trust;
- arranging appropriate training and guidance to support staff in meeting their duties under data protection law;
- supporting the DPO in investigating personal data;
- supporting the DPO in responding to information requests.

4.5 Headteachers

Headteachers are responsible for:

- providing day-to-day leadership on data protection issues within their Academies;
- ensuring all staff fulfils their duties around data protection; and
- ensuring all their staff complete any training arranged by the Academy or Trust.

4.6 All Staff

All staff are responsible for:

- processing personal data in accordance with this policy, any associated guidance and any supplementary procedures issued by Data Protection Leads;
- handling records containing personal data in secure manner and in accordance with the Trusts acceptable use of ICT policy;
- treating information in a confidential manner and respecting the privacy and information rights of individuals whose personal data you are given access to;
- recording personal data accurately, in a timely manner using appropriate Trust systems;
- not sharing personal data with individuals, external agencies, suppliers, or other organisations, unless required and appropriate Line Manager approval has been sought in advance;
- seeking advice from the Data Protection Officer prior to sharing personal data with any new providers of services or online resources for learners
- informing their Line Manager about any relevant changes to their own personal data, such as a change of address, other contact details, or emergency contact information;
- fully participating in all data protection training arranged for them, including familiarising themselves with any updated guidance that is issued by Data Protection Leads
- cooperating with any reasonable request for involvement in compliance monitoring;
- reporting any personal data breach for which they are responsible, as soon as they become aware of it, in accordance with section 12 of this policy; and
- notifying their Data Protection Lead or DPO if they:
    - have any questions about the operation of this policy or data protection law;
    - have any concerns that this policy is not being followed;
    - are unsure whether they can use personal data in a particular way; or
    - receive a request from an individual to exercise their rights, in accordance with section 11 of this policy.

4.7 The Information Commissioner's Office (ICO)

The ICO are the UK data protection supervisory authority. They are responsible for upholding information rights, promoting openness by public bodies and data privacy for individuals. They also hold Data Controllers to account in respect of the processing of personal data.

Matrix Academy Trust is registered as a Data Controller with the ICO. Our registration number is: ZA185164

5. Collecting personal data

We will only collect personal data where we have identified and documented a lawful basis on which to do so. For special categories of personal data, we will meet both a lawful basis and a condition outlined within data protection law to allow that data to be processed.

For criminal offence data, we will meet both a lawful basis and a condition outlined within data protection law.

Whenever we collect personal data, we will explain to the data subject why this information is needed. We will usually do this by publishing a Privacy Notice. Our Privacy Notices will explain why using personal data is necessary, what the information will be used for (the purpose) and whether it will be shared.

We will only collect the personal data that is necessary to fulfil the purposes for which it is required.

In the event we intend to use personal data for a purpose that differs from the one for which it was originally collected, we will inform the data subject before such processing takes place or we will seek consent where necessary.

6. Storing personal data

We will protect the confidentiality, integrity and availability of the personal data we process. That is:

- only people who are authorised to use the data will be allowed to access it (confidentiality);
- the data will be kept accurate and up-to-date (integrity); and
- the data will be stored on systems and devices approved by Trust – to ensure all authorised users will be able to access it for authorised purposes (availability).
- Staff should not store personal data on their own equipment or personal devices (computers, mobile devices, portable and removeable storage)
- Portable storage devices, including memory sticks, SD cards and portable hard-drives are not to be used (even where these devices are encrypted).

We will take appropriate organisational and technical steps to minimise the risk that personal data is lost, damaged or accessed without authorisation. Such measures will include, for example:

- entry controls to restrict physical access to areas in which personal data is stored;
- locking active user sessions on computers and other devices, when equipment is left unattended;
- user-level or role-based permissions to control access to systems and electronic records;
- email and file encryption to protect the sharing and transfer of electronic records;
- secure, lockable storage facilities for paper records;
- compliance checks undertaken by the DPO where new systems or processes are used which involve the processing of personal data
- additional checks undertaken where processing of personal data involves higher risk, including where sensitive personal data is used. In this case a Data Protection Impact Assessment may be required
- Identifying where AI technology is used to processed personal data and conducting appropriate risk assessments prior to use
- regular review of our ICT infrastructure and staff working practice to limit the threat of cyber security attacks
- secure, offsite backups that enable lost or damaged data to be restored;
- regular data-checking exercises to ensure data is accurate and up-to-date; and
- regular training to ensure staff are aware of our expectations for good practice.

Staff can find details about their obligations relating to data security in:

- the staff code of conduct;
- the staff guidance distributed by Data Protection Leads; and
- the staff ICT acceptable use policy.

7. Sharing personal data

We may share personal data with any staff member within the Trust or any of its Academies, where a lawful basis is identified. This includes where it is necessary to support teaching and learning, required to support the performance of school safeguarding duties, required to fulfil a legal obligation, or where we have obtained explicit written consent from the individual and data relates to the data subject. If at any time you are unsure whether data sharing is lawful or appropriate, staff are required to check with the Data Protection Officer prior to sharing

We share personal data with other organisations in order to carry out our functions. This includes, but is not limited to, where:

- we use a third-party suppliers or systems to support the delivery of teaching and learning or pastoral support in our academies;
- we are required to complete a data return to another public sector organisation, such as the Department for Education; and
- we need to report a serious concern about the safety of our pupils or staff.

We will take appropriate organisational and technical steps to ensure personal data is shared securely. Such measures will include, for example:

- data processing agreements for any third parties who process personal data on our behalf;
- passwords to restrict access to electronic files;
- encryption to protect email contents (particularly those to external organisations); and
- pseudonymisation or anonymisation, where this would not undermine the processing.

Where we transfer personal data internationally, we will do so in line with data protection law.

8. Disposing of personal data

We will only retain personal data for as long as we need it in order to fulfil the purposes for which it was processed. Matrix Academy Trust will maintain a retention schedule to outline how long we will keep different types of personal data.

A record of disposals will also be maintained by each academy

Once personal data is no longer needed, we will dispose of it securely. Disposal methods include:

- onsite or secure offsite shredding for paper records;
- deleting or overwriting electronic records; and
- physical destruction of redundant devices, drives, disks and other media.

9. Photographs and videos

We take photographs and record images of individuals within and around our premises, as well as some other situations such as during trips. We do this for various purposes, including to:

- identify pupils in order to operate certain systems and services, such as school meals;
- identify staff and visitors to our premises so that we know who is permitted to be on-site;
- celebrate pupils' work and school life within our Academies;
- evidence the learning and development achieved by our pupils;
- help showcase the Academies as part of our marketing and promotional materials; and
- operate our CCTV systems.

We will obtain written consent before we publish an individual's image externally, including as part of our marketing and promotional materials, unless we are otherwise licensed to use the image for such a purpose.

Where consent is required in relation to a pupil's image, we will request it from their parent/carer. However, for a pupil aged 16 or older, we may request consent from the pupil directly.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will take reasonable steps to cease using the image as part of our marketing and promotional materials.

Any photographs or videos taken by parents/carers at academy events for their own personal

use are not covered by data protection law. However, for safeguarding reasons, parents and attendees of publicly accessible school events, should be notified about the appropriate use of such images. This should include notices or announcements explaining that images taken by attendees should not be shared publicly – particularly on social media where accounts are not private.

For other purposes, however, consent to use people's images may not be required.

We use CCTV in various locations at our academies around school site to ensure the security of our buildings, assist staff in the undertaking of statutory safeguarding duties and support academies' behaviour policies.

We will adhere to the ICO's code of practice 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 there is prominent signage around site.

Any enquiries about the CCTV system should be directed to the Headteacher in the first instance.

We will maintain a separate policy relating to the operation of our CCTV systems.

10. Biometric recognition systems

Some of our Academies use biometric recognition systems. These systems use technology for identification purposes (for example, in our secondary academies, pupils may use fingerprints to receive school dinners instead of paying with cash). Where we use biometric systems, we will comply with the requirements of the Protection of Freedoms Act 2012.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

10.1 Parents/carers and pupils

Parents/carers will be notified before any new biometric recognition system is put in place, or before their child's personal data is processed as part of it. We will request written consent from at least one parent/carer before we collect biometric data from their child.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

10.2 Staff

Staff will be notified before any new biometric recognition is put in place. We will request written consent before we collect their biometric data.

Staff can decide against using any biometric recognition system we operate. Where consent is given to opt in, that consent can be withdrawn at any time.

11. Rights of data subjects

We are committed to upholding individuals' rights under data protection law.

It is important to understand that not all of these rights apply at all times. However, we will ensure all requests to exercise a right are always considered fairly and lawfully.

We may need to ask for identification from the person making the request before we act upon it.

11.1 Right to be informed

People have the right to be informed about what personal data we collect about them and how we use it. We will uphold this right by:

- providing data subjects with the relevant privacy notice at the time we collect their personal data, unless this information has already been given to them or it would be otherwise unreasonable to provide it.
- Privacy Notices will be published on our Trust and Academy websites.

11.2 Right of access (subject access)

People have the right to access their personal data. We will uphold this right by:

- providing information on our websites and Privacy Notices about how to make a subject access request;
- ensuring staff are able to recognise such a request
- Maintaining a clear process for the handling of information requests
- Regularly reviewing the storage of records containing personal data to minimise data retention and limit the time required for responded to requests;
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported; and
- Clarifying requests as appropriate to confirm which records are to be considered
- Reporting requests to the Data Protection Officer without delay

11.3 Right to rectification

People have the right to have their personal data corrected if it is inaccurate, or completed if it is incomplete. We will uphold this right by:

- conducting regular data-checking exercises to give people the opportunity to identify inaccurate data;
- ensuring staff are able to recognise a request to amend personal data;
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported; and
- Reporting requests to the Data Protection Officer without delay

11.4 Right to erasure

People have the right to have their personal data erased in certain circumstances. We will uphold this right by:

- ensuring staff are able to recognise a request to erase personal data; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported;
- Reporting requests to the Data Protection Officer without delay

11.5 Right to restrict processing

People have the right to request that we limit how we use their data in certain circumstances. We will uphold this right by:

- ensuring staff are able to recognise a request to restrict processing; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported

- Reporting requests to the Data Protection Officer without delay.

11.6 Right to data portability

People have the right to obtain and reuse their personal data across different services by copying or transferring it between systems in a secure way. We will uphold this right by:

- ensuring staff are able to recognise a request for data portability; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported.
- Reporting requests to the Data Protection Officer without delay

11.7 Right to object

People have the right to object to the processing of their personal data in certain circumstances. We will uphold this right by:

- ensuring staff are able to recognise a request for objecting to processing; and
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported
- Reporting requests to the Data Protection Officer without delay.

11.8 Rights related to automated decision-making, including profiling

People have the right not to be subject to a decision based solely on automated processing, including profiling, which has a significant affect upon them. We will uphold this right by:

- informing people, as part of our privacy notices, about any processing activity that uses automated decision-making and/or profiling;
- Identifying new systems or processes which involved the use of AI including the use of generative AI tools to support teaching and learning, or where AI is embedded into administrative and management systems.
- completing a data protection impact assessment for any processing activity that is based solely on automated processing, including profiling, and implementing any agreed actions that arise from any such assessment (see section 13);
- ensuring staff are able to recognise a request made under this right;
- appointing particular staff members to co-ordinate the responses to such requests, and ensuring those staff members are properly trained and supported; and
- Reporting requests to the Data Protection Officer without delay

11.9 Parental requests to see the educational record

- Parents, or those with parental responsibility, can request to access to their child's educational record (which includes most information about a pupil). The academy should make this information available within 15 school days of receipt of a written request.

- Academies are not legally obliged to provide this information. However, this will be determined on an individual case by case basis.

- Where it is not clear that a request relates solely to accessing educational records, advice should be sought from the DPO prior to disclosure.

12. Personal data breaches

We will take all reasonable steps to minimise the risk of a personal data breach. However, where a

data breach does occur, it is important that staff are open and honest about it so that it can be managed quickly.

On discovering or causing a breach, or potential breach, the staff member must report it immediately to their Data Protection Lead and Data Protection Officer using the relevant academy email address below:

DPO@matrixacademytrust.co.uk – Matrix Academy Trust Head Office
DPO@barrbeaconschool.co.uk - Barr Beacon School
DPO@decschool.co.uk – Dame Elizabeth Cadbury
DPO@etonecollege.co.uk – Etone College
DPO@bloxwichacademy.co.uk – Bloxwich Academy
DPO@tgbs.co.uk – Turves Green Boys' School
DPO@smestowacademy.co.uk – Smestow Academy
DPO@wednesfieldacademy.co.uk – Wednesfield Academy

Breaches that occur at an Academy will normally be investigated by the DPO and Data Protection Lead for that Academy. However, if this would create a conflict of interest, the investigation will be completed by the DPO and the Trust. Breaches that occur elsewhere within the organisation, or which are caused by a data processor, will be also be investigated by the DPO and the Trust.

All breach investigations will:

- assess the likely risk to individuals as a result;
- determine the cause of the issue
- recommend any actions that might be taken to mitigate that risk; and
- reflect on how to reduce the likelihood that a similar breach will occur in future.

In the event that the investigation finds a risk to rights of individuals is likely, we will report the breach to the ICO. Where feasible, we will do this within 72 hours; otherwise, we will do this without undue delay. Any such reports will be completed by our Data Protection Officer.

In the event that the investigation finds a risk to individuals is high, we will notify those individuals directly and without undue delay.

We will record all personal data breaches, including those that are not reported to the ICO.

13. Data protection impact assessments

In the event we plan to introduce a new data processing activity, or that we plan to change the way any existing processing is conducted, we will consider whether to carry out an impact assessment. We will maintain a screening tool to ensure this is considered consistently across the Trust.

It is the Project Lead's responsibility to ensure that the DPO is notified in the early stages of any project that involves personal data.

Where the DPO decides an impact assessment should be carried out, it will be completed during the project planning stage *before* any decisions are made about whether to approve the processing. This will allow us to identify the associated data protection risks early enough that we can act to minimise them.

14. Training and support

We are committed to supporting our staff to meet their duties relating to data protection. Accordingly, we expect all staff to complete:

- a mandatory induction in data protection when they join the organisation, which will include:
  - an essential overview of basic data protection;
  - the detailed guidance about our expectations for good practice; and
  - a copy of this policy; and
- mandatory annual refresher training.

We will keep a record of the mandatory training completed by our staff.

Staff will have ongoing access to training materials in case they would like to refresh their own understanding of the content.

Staff will also have access to key people in case they have any questions about data protection or any concerns about poor practice.

15. Monitoring and review

The Data Protection Officer will independently monitor our compliance with this policy – and with data protection law more broadly – on an annual basis. Independent monitoring will include:

- site walks to identify any examples poor practice to address, or good practice to share;
- interviews to assess the level of understanding among staff and to identify any potential training requirements;
- a review of any data breaches to assess how they were handled and learned from; and
- a scheduled audit of compliance at Academy level

The results of independent monitoring will be reported directly to the Trust Board and circulated to the Data Protection Leads for each Academy.

The Trust, Data Protection Leads, and Governance Advisory Boards may carry out additional monitoring at their discretion.

This policy will be reviewed by the Trust Board every two years, or else following any proposal to change to its content significantly.