Data Protection Policy

Applicable to:	✓	All individual academies within NEAT Academy Trust
	×	Specified academies only within NEAT Academy Trust
	✓	Central team within NEAT Academy Trust
	✓	NEAT Active Ltd
Approval body:	NEAT Academy Trust Board of Directors, which may be delegated NEAT Active Ltd Board of Directors, which may be delegated	

Status:

Statutory policy or document	No
Review frequency	As determined by the Boards
Approval by	As determined by the Boards

Publication:

Statutory requirement to publish on website	No
If not, agreed to publish on website?	Yes – Trust

Version Control:

Revision Record of Issued Versions			
Author	**Creation Date**	**Version**	**Status**
Central Support Manager (SH)	24 May 2018	1.0	Agreed by Board of Directors for implementation across the Trust.
Changed by	**Revision Date**	**Version**	**Status**
Director of HR and Governance (SH)	10 April 2019	2.0	Minor amendments to spelling, punctuation and grammar.
Governance Support Manager (HH)	11 December 2020	3.0	Amended version agreed by Executive Team to reflect updated guidance from ICO about charging for SARs
Governance Support Adviser (HH) and Head of Governance and Corporate Affairs (SH)	26 March 2021 To apply from 01.04.21	4.0	Amended to become joint policy for NEAT and NEAT Active Ltd and to include special category data policy. Approved by Exec Team on behalf of NEAT Academy Trust Board. Approved by Executive
Head of Governance and Corporate Affairs (SH)	12 April 2021	5.0	Very minor amendment to DPO contact details.

Review Date	
Frequency	**Next Review Due**
Every three years	March 2024 (or earlier if new guidance or legislation issued and/or business need for earlier review identified)

1 Purpose

The purpose of this policy is to set out how we protect the personal data that we hold in relation to pupils, parents, employees, job applicants, members, non-executive directors/trustees, local governors, volunteers and customers and how we deal with requests in relation to that data.

2 Scope

This policy applies to both NEAT Academy Trust and its subsidiary company, NEAT Active Ltd, (the NEAT Group).

It covers information in all forms including, but not limited to:

- hard copy or documents printed or written on paper;
- information or data stored electronically, including scanned images;
- communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- speech, voice recordings and verbal communications, including voicemail;
- published web content, for example intranet and internet; and
- photographs and other digital images.

3 Policy statement

We will ensure that personal data is processed in accordance with the requirements of data protection legislation and that we comply with the principles specified in the legislation that data will 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 they are processed;
- accurate and, where necessary, kept up-to-date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- 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.

4 Legal considerations

This policy is designed to comply with the requirements of the Data Protection Act 2018, associated guidance and Codes of Practice issued under the legislation. Schedule 1 of the Act requires data controllers to have in place an ‘appropriate policy document’ for the processing of special categories of personal data and criminal convictions data.

5 Roles and responsibilities

- **NEAT Academy Trust and NEAT Active Ltd Boards of Directors:** The Boards will review this policy and evaluate its effectiveness. The trust's Audit and Risk Committee has oversight of any risks arising from information governance.

- **Information asset owners (IAO):** An IAO is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. IAOs will be appointed based on sufficient seniority and level of responsibility. IAOs are responsible for the security and maintenance of their information assets. This includes ensuring that all colleagues are using the information safely and responsibly. They will also determine the retention period for the asset, and when destroyed, ensure this is done so securely.

- **Data Protection Officer (DPO):** The Data Protection Officer appointed for the NEAT Group is: Veritau Ltd, Information Governance Team, County Hall, Racecourse Lane, Northallerton DL7 8AL Tel: 01609 554025 E-mail: schoolsDPO@veritau.co.uk . The DPO is a statutory position and operates in an advisory capacity. Duties include:
  - acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
  - facilitating a periodic review of the corporate information asset register and information governance policies;
  - assisting with the reporting and investigation of information security breaches;
  - providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
  - reporting to non-executive directors/trustees on the above matters.

- **Governance Support Adviser:** The Governance Support Adviser is responsible for responding to requests from data subjects under this policy, providing advice and guidance to staff, governors and non-executive directors/trustees about data protection matters and liaising with the Data Protection Officer appointed for the NEAT Group.

- **All employees and authorised agents acting on behalf of NEAT Academy Trust or NEAT Active Ltd:** have a duty to ensure they recognise and deal with data subject access requests in accordance with this policy.

6 Information asset register

The DPO will provide advice on developing and maintaining an Information Asset Register (IAR) for the trust, its academies and NEAT Active Ltd. The register will include the following information for each asset:

- an individual information asset identification number;
- the owner of that asset;
- description and purpose of the asset;
- whether there is a privacy notice published for that asset;
- format and location of the asset;
- which officers (job titles/teams) have routine access to the information;
- whether there are any data sharing agreements relating to the information and the name of that agreement;

- conditions of data processing;
- details of any third parties contracted to process the information; and
- retention period for the asset.

The IAR will be reviewed at least annually and we will inform the DPO of any significant changes to the information assets as soon as possible.

7 Training

We will ensure that appropriate guidance and training are given to relevant colleagues, volunteers, non-executive directors/trustees, governors and other authorised school/service users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

We will consult the DPO in relation to training, where necessary, to ensure training resources and their implementation are effective.

We will ensure that any third party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

8 Privacy notices

We will provide a privacy notice to data subjects each time we obtain personal information from or about that data subject.

We provide the following privacy notices:

- the main privacy notice relating to data about pupils and parents of NEAT Academy Trust will be displayed on the trust's website in an easily accessible area with links from each academy's website. This notice will also be provided in a hard copy to new pupils and parents at the start of the school year as part of their information pack. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects);
- a privacy notice for customers/service users of NEAT Active Ltd;
- a privacy notice for external delegates participating in professional development provided by the trust;
- privacy notices for job applicants will be displayed on websites;
- privacy notices for employees will be provided at the start of their employment; and
- privacy notices for members, non-executive directors/trustees and local governors will be provided at commencement of their term of office.

Privacy notices will be cleared by the DPO prior to being published or issued. We will keep a record of privacy notices on the Information Asset Register.

9 Information sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for us to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notices (as above). Any ad hoc sharing of information will be done in compliance with our legislative requirements.

10 Data Protection Impact Assessment (DPIAs)

We will conduct a data protection impact assessment for all new projects involving high risk data processing, as defined by the Data Protection Act 2018. This assessment will consider the privacy risks and implications of new projects, as well as providing solutions to the identified risks.

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, providing relevant advice.

11 Retention periods

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition, IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods. We maintain a document retention schedule that sets out how long specific documents are retained.

12 Destruction of records

Retention periods for records are recorded in our IARs. When a record reaches the end of its retention period, the IAO will arrange for the records, both electronic and paper, to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins. Advice in regards to the secure destruction of electronic media will be sought from relevant IT support.

A record should be retained of all files destroyed including, where relevant:

- file reference number;
- description of file;
- date of disposal;
- method of disposal and
- staff member who destroyed record.

13 Third party processors

All third party contractors who process data on our behalf must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.

If any data processing is going to take place outside of the European Economic Area (EEA) then the DPO must be consulted prior to any contracts being agreed.

A member of the trust's Executive Team may insist that any data processing by a third party ceases immediately if it believes that the third party has not got adequate data protection safeguards in place.

14 Data subject access requests

Requests by data subjects to access the data we hold about them should be made to the Governance Support Adviser.

However, any member of staff, governor or non-executive director/trustee may receive a request for an individual's personal information. This must be passed on to the Governance Support Adviser without delay.

The Governance Support Adviser will log each request and acknowledge it within five working days.

Whilst the Data Protection Act 2018 does not require such requests to be made in writing, applicants are encouraged where possible to do so and we provide a form for this purpose on the trust's website. Any applicant who requires assistance should seek help from the trust.

The Governance Support Adviser must be satisfied as to the applicant's identity and may have to ask for additional information such as:

- valid photo ID (driver's licence, passport etc);
- proof of address (utility bill, council tax letter etc);
- further information to be satisfied of the applicant's identity.

Only once the Governance Support Adviser is satisfied of the applicant's identity and has sufficient information on which to respond to the request will it be considered valid. They will then respond to the request within one month of receipt.

We can apply a discretionary extension of up to two months to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If we wish to apply an extension we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first month of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads.

We may charge a 'reasonable fee' for the administrative costs of complying with a request if:

- it is manifestly excessive; or
- an individual requests further copies of their data following a request.

In very limited cases we may also refuse a request outright as 'manifestly excessive' if we would have to spend an unjustified amount of time and resources to comply. Requests which are judged to be 'manifestly unfounded' will also be refused outright.

Should we think any charges, refusals or exemptions are necessary to apply we will seek guidance from our DPO to discuss their application.

If a subject access request is made by a parent whose child is 12 years of age or over, we may consult with the child or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

15 Other data subject rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the Data Protection Act 2018 including:

- right to rectification;
- right to erasure;
- right to restrict processing; and

- rights in relation to automated decision making and profiling.

Whilst the Data Protection Act 2018 does not require such requests to be made in writing, applicants are encouraged where possible to do so. Any applicant who requires assistance should seek help from the trust.

Requests should be forwarded to the Governance Support Adviser who will acknowledge the request and respond within one month. Advice regarding such requests will be sought from the DPO.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

16 Complaints

You can submit a complaint under the NEAT Academy Trust or the NEAT Active Ltd Complaints Policy and Procedure if your request as a data subject is refused or you are dissatisfied with how it has been handled and ask us to undertake an internal review.

Any individual who wishes to make a complaint about the way we have handled their personal data should contact our appointed Data Protection Officer at the address provided in section 5 above.

General

This policy is at the discretion of the boards of directors and can be varied at any time. In the event of any conflict with primary legislation or statutory regulations, the legal provisions will have precedence over this policy in all cases.

Appendix 1: Special Category Data

Introduction

NEAT Academy Trust and NEAT Active Ltd process special category and criminal conviction data in the course of fulfilling their functions. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This appendix to the Data Protection Policy fulfils this requirement.

This policy complements existing records of processing held by NEAT Academy Trust and NEAT Active Ltd as required by Article 30 of the General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces the existing retention and security policies, procedures and other documentation in relation to special category data.

Scope

We are committed to the protection of all special category and criminal convictions data that we process. This policy applies to all such data, whether or not an appropriate policy document is required.

Special categories of data processed

We process the following special categories of data

- racial or ethnic origin;
- religious or philosophical beliefs;
- trade union membership;
- health;
- sexual orientation;
- Biometric identifier.

We also process criminal convictions data for the purposes identified below.

NEAT Academy Trust and NEAT Active Ltd rely on the following processing conditions under Article 9 of the General Data Protection Regulation and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

Purposes	Examples of use (not exhaustive)	Processing conditions
For the provision of education to pupils, including providing support to pupils who are recognised as having Special Educational Needs.	The use of special category data to identify pupils who require additional support.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To ensure the safety and wellbeing of pupils	Details of safeguarding concerns held in safeguarding files. Allergy and disability information.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For identification/ authentication	Biometric (fingerprint) school meal payments.	Article 9 (2)(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
To monitor pupil attendance	Medical reasons for absence.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the provision of school trips	Provision of dietary requirements to third parties involved with facilitating the school trip.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
For the provision of education in respect of Looked After Children.	Details of criminal convictions in respect of child's parents.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes.
The management of staff	Personnel files identify medical reasons for absences. Handling of disciplinary proceedings and grievances.	Article 9(2)(b) Employment, social security and social protection Schedule 1 Part 1, 1(a) Processing necessary for the purposes of carrying out obligations and exercising specific rights of the controller and or data subject in the field of employment
To undertake recruitment and pre-appointment checks	DBS certificates (until a decision is made in respect of their appointment). Self-disclosed details of criminal convictions of job applicants and employees.	Article 9(2)(b) Employment, social security and social protection Schedule 1 Part 1, 1(a) Processing necessary for the purposes of carrying out obligations and exercising specific rights of the controller and or data subject in the field of employment.
To facilitate the functioning of the governing body	Governors will use special category data where applicable when considering solutions to, for	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes

Purposes	Examples of use (not exhaustive)	Processing conditions
	example, access to school for a disabled student.	
For the prevention and detection of crime	Potential special category and criminal offence data shared	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 5 (10). Preventing or detecting unlawful acts
The handling of complaints	Complaint investigations may involve reference to and use of special category/ criminal conviction data where applicable to the content and nature of the complaint.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To fulfil legislative health and safety requirements	Pupil and employee health information for assessment of reasonable adjustments.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes
To monitor equality and diversity	Collection of employee and pupil race, ethnicity and religious background. Collection of employee sexual orientation and gender reassignment.	Article 9(2)(g) Substantial public interest Schedule 1, Part 2, 6 (2) statutory and government purposes

Compliance with Article 5 – The Data Protection Principles

We maintain documentation and implement procedures which ensures compliance with the Data Protection Principles under Article 5 of the General Data Protection Regulation.

Document/ procedure	Principles	How documents and procedures aid compliance
Privacy notices	Accountability Lawfulness, fairness and transparency Purpose limitation Accuracy Storage limitation	We publish a suite of privacy notices which stipulate that the trust/company is the 'data controller', the purposes for which the trust/company processes special category data and the lawful bases we rely on to do this. This fulfils our duty to be transparent about the data that we hold, how it is processed and that the trust/company as the data controller is accountable.

Document/ procedure	Principles	How documents and procedures aid compliance
	Data minimisation	All privacy notices provide details of how to make a data rights request, ensuring that data subjects are able to check and challenge the lawfulness and accuracy of the data processed. Privacy notices are updated where the trust/company makes changes to the way it processes personal data.
Policies	Accountability Purpose limitation Storage limitation Security Accuracy Data Minimisation	We maintain a framework of information governance policies which detail the expectations and responsibilities of employees of the trust/company. This includes, but is not limited to, the following policies: • Personal Data Breach Procedure • Acceptable Use Policy • Surveillance Policy These policies set out the processes in place to ensure that the purposes and duration for which special category data are held are not exceeded and the security mechanisms and procedures that are in place to keep this information secure. Administrative procedures for ensuring personal data is recorded accurately and kept up to date are also documented. These policies are reviewed regularly in line with the trust/company's policy review schedule to ensure the processes, procedures and measures remain appropriate and effective.
Information Asset Register	Lawfulness, fairness and transparency Purpose limitation Security	Maintenance of this document fulfils the trust/company's legal obligation under Article 30 of the General Data Protection Regulation to keep a record of its processing activities. Information assets which contain special category data have been identified and Article 6, Article 9 and Schedule 1 conditions (where applicable) have been identified for each asset. Retention periods for each asset, based on the trust/company's retention schedule, have also been identified, along with the technical and organisational security measures that are in place to protect each asset.

Document/ procedure	Principles	How documents and procedures aid compliance
		This document is reviewed regularly and updated where there have been changes to the trust/company's data processing.
Data Protection Impact Assessments (DPIAs)	Accountability Lawfulness fairness and transparency Purpose limitation Data minimisation Accuracy	We conduct Data Protection Impact Assessments where we are undertaking new, high risk processing, or making significant changes to existing data processing. The purpose of the DPIA is to consider and document the risks associated with a project prior to its implementation, ensuring data protection is embedded by design and default. All of the data protection principles are assessed to identify specific risks. These risks are then evaluated and solutions to mitigate or eliminate these risks are considered. Where a less privacy-intrusive alternative is available, or the project can go ahead without the use of special category data, the trust/company will opt to do this. All DPIAs are signed by the trust/company Senior Information Risk Owner and Data Protection Officer.
Mandatory data protection training	Accountability Security	All staff undertake mandatory data protection training, which is refreshed every 2 years. Staff members who have particular responsibility for managing the risks to personal data, such as the Senior Information Risk Owner, Specific Point of Contact and Information Asset Owners, undertake additional specialist training where applicable. Where new processes are introduced as a result of additions to or changes to processing, additional training will be provided to staff members involved with the project. The requirement for this will be identified as part of Data Protection Impact Assessments.
Retention schedule and destruction log	Purpose limitation Data minimisation	We do not retain special categories of data for any longer than it is necessary to do so in order to fulfil our specific purposes. The trust/company has a retention schedule in place which is based on guidance issued by the Information and Records Management Society (IRMS). Where there is no legislative or best practice guidance in place, the Senior Information Risk Owner will decide how long the information should be retained based on the necessity to keep the information for a

Document/ procedure	Principles	How documents and procedures aid compliance
		legitimate purpose or purposes. The Information Asset Owner has responsibility for ensuring records retention periods are adhered to. The trust/company also maintains a destruction log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed.
Technical and organisational security measures and procedures. Recording and reporting personal data breaches where necessary	Security Accountability Accuracy	We employ the following technical and organisational security measures where appropriate to protect the personal and special category data that the trust/company processes • Password protection of electronic devices and systems • Encryption of portable devices • Encryption of emails when personal data is sent outside the trust/company • Recorded delivery of sensitive paper documents • Secure, fireproof storage of paper records using a key/ PIN management system • Clear desk policy • Audit trails on electronic systems • Regular backups that can be restored in the event of an emergency • Access/ permission controls • Secure destruction of paper records • Information governance policies (detailed above) • Physical building security measures (locked doors, visitor sign in procedure alarm system, CCTV etc.) • Cyber security risk prevention measures (firewalls and anti-virus software, phishing email awareness, download restrictions etc.) In the event that these measures should fail and a personal data breach occurs, the incident will be recorded in a log, investigated and reported to the Data Protection Officer where necessary. Severe incidents are reported to the Information Commissioner's Office. This process is documented in greater detail in the Personal Data Breach Procedure referred to above.

Document/ procedure	Principles	How documents and procedures aid compliance
Written contracts with data processors	Accountability Security	When we share personal data with a data processor, a written contract is obtained. All existing contracts are checked to ensure that all mandatory data protection clauses are present and all new contracts are assessed prior to forming an agreement with the processor.
Compliance with data rights requests	Lawfulness, fairness and transparency Accountability Accuracy	We maintain a log of all data rights requests and have appropriate processes set out in the trust/company's policies for handling such requests.
Data Protection Officer	Accountability	We have appointed a Data Protection Officer to oversee the trust/company's compliance with the data protection principles.

Retention of special category and criminal convictions data

The retention periods of special category and criminal convictions data are set out in the trust/company's retention schedule, which is based on the Information and Records Management Society (IRMS) Toolkit for Schools. Retention periods of specific information assets are identified in the trust/company's information asset register.