Data Protection Policy

Applicable to:	✓	All individual academies within NEAT
	×	Specified academies only
	✓	NEAT Trust
Approval body:	NEAT Board of Directors	
Effective date:	24 May 2018	

Status:

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

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	1.1	Minor amendments to spelling, punctuation and grammar.

Review Date	
Frequency	**Next Review Due**
Every three years	May 2021 (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, staff, job applicants, directors/trustees, local governors and customers and how we deal with requests in relation to that data.

2 Scope

The policy applies to the trust and all of its academies. It applies to 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 to ensure that we comply with the requirements of the Data Protection Act 2018, associated guidance and Codes of Practice issued under the legislation.

5 Roles and responsibilities

- **Trust's Board of Directors:** The Trust Board will review this policy and evaluate its effectiveness. The Audit, Risk and Finance 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. The trust and its academies will ensure that IAOs are

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 other members of staff are using the information safely and responsibly. They will also determine the retention period for the asset, and when destroyed, ensuing this is done so securely.

- **Data Protection Officer (DPO):** The Data Protection Officer appointed by the trust is: Veritau Ltd, Information Governance Team, County Hall, Racecourse Lane, Northallerton DL7 8AL Tel: 01609 532526 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 directors/trustees on the above matters.

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

6 Information asset register

The DPO will advise the trust in developing and maintaining an Information Asset Register (IAR) for the trust and its academies. 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;
- retention period for the asset

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

7 Training

We will ensure that appropriate guidance and training are given to relevant staff, volunteers, directors/trustees, governors and other authorised school 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 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 job applicants will be displayed on the trust's website;
- a privacy notice for employees will be provided at commencement of their employment with the trust; and
- a privacy notice for 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 trust's 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 Data Protection Officer must be consulted prior to any contracts being agreed.

A member of our Executive Team may insist that any data processing by a third party ceases immediately if it believes that that 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 trust's Governance Support Adviser.

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

The trust's 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. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.

Should we think any 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 trust's 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 trust's 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
In the event of any conflict with primary legislation or statutory regulations, the legal provisions will have precedence over this policy in all cases.