Northern Education Trust

Outcomes Focused, Child Centred

General Data Protection Regulation (GDPR) Policy

Date approved by NET:	22nd June 2018
Next Review Date:	June 2020

NORTHERN EDUCATION TRUST (NET)

General Data Protection Regulation (GDPR) Policy

DATA PROTECTION

1.0 Introduction

1.1 Northern Education Trust ("the Trust") collects and uses certain types of personal information about employees, students, parents and other individuals who come into contact with the Trust and its academies in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and other related legislation.

1.2 This policy will be reviewed at least every 2 years.

2.0 Personal Data

2.1 The GDPA and DPA apply to computerised and paper-based personal data.

2.2 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier, such as:

- A name;
- An identification number;
- Location data;
- An online identifier; or
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.3 The GDPR does not cover paper records unless they are part of a 'filing system'. However, under the Data Protection Act 2018 (DPA 2018) unstructured manual information processed only by public authorities constitutes personal data. This includes paper records that are not held as part of a filing system. The aim is to ensure that such information is appropriately protected for requests under the Freedom of Information Act 2000.

2.4 Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. Special category data is information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

2.5 Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

2.6 The law requires the Trust to collect special categories of data. The Trust will only process special category personal data if:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

2.7 Sometimes the Trust needs consent to collect and use personal information. Where this is the case, the Trust will make clear that it needs consent when it collects the information and that consent can by withdrawn at any time.

2.8 Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

3.0 The Data Protection Principles

3.1 The GDPR sets out seven key principles that personal data shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d. Accurate and, where necessary, kept up to date ('accuracy');
e. 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 ('storage limitation');
f. 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 ('integrity and confidentiality');

3.2 The seventh principle is that the controller is responsible for, and can demonstrate compliance with, the other principles ('accountability')

3.3 These principles lie at the heart of the Trust's approach to processing personal data. The Trust will:

- Inform individuals as to the purpose of collecting any information from them, as and when it asks for it;
- Be responsible for checking the quality and accuracy of the information;
- Regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;
- Ensure that when information is authorised for disposal it is done appropriately;
- Enforce appropriate security measures to safeguard personal information whether it is held in paper files or on computer systems, and follow the relevant security policy requirements at all times;

- Share personal information with others only when it is necessary and legally appropriate to do so;
- Set out clear procedures for responding to requests for access to personal information known as subject access requests; and
- Report any breaches of the GDPR in accordance with the procedure in paragraph 18 below.

4.0 Lawful bases for processing

4.1 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever The Trust processes personal data:

a. **Consent**: the individual has given clear consent to process their personal data for a specific purpose;
b. **Contract**: the processing is necessary for a contract with the individual, or because they have requested specific steps before entering into a contract;
c. **Legal obligation**: the processing is necessary to comply with the law (not including contractual obligations);
d. **Vital interests**: the processing is necessary to protect someone's life;
e. **Public task**: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law;
f. **Legitimate interests**: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to a public authority processing data to perform official tasks.)

5.0 Use of personal data by the Trust and Academies

5.1 The Trust holds personal data on students, staff and other individuals such as visitors. In each case, the personal data is processed in accordance with the GDPR and DPA principles

6.0 Student data

6.1 The law requires the Trust to collect personal information relating to children and their families. The Trust does this using information:

- From the local authority and taken from the applications made for an Academy place;
- From previous schools;
- From the Department for Education (DfE); and
- Given directly by parents, carers and students

6.2 The Trust also collects information to perform the public task of running its academies.

6.3 The personal information the Trust collects includes:

- Name, address, date of birth;
- Characteristics, including ethnicity, language, nationality, country of birth and free school meal eligibility;
- Attendance information;

- Assessment information based on National Curriculum and informal test results and teacher assessments;
- Relevant medical information;
- Information relating to special educational needs and disabilities (SEND);
- Behaviour and effort information;
- Photographs for use within the Academy, including photographs of individual students used for identification and safeguarding and photographs of activities for use in educational progress monitoring on internal displays; and
- Video using closed circuit television (CCTV cameras) captured from cameras mounted around the Academy and used only for the purpose of site security and safeguarding children

6.4 The Trust collects information about children and their families to:

- Support student learning;
- Monitor and report on student progress;
- Provide appropriate pastoral care;
- Assess the quality of service;
- Comply with the law regarding data sharing;
- Protect student welfare; and
- Safeguard children.

7.0 Staff data

7.1 The Trust collects and uses personal information about staff only when the law allows it to. Most commonly, The Trust processes data where it needs to:

- Fulfil a contract entered into with staff;
- Comply with a legal obligation; or
- Carry out a task in the public interest.

7.2 Less commonly, the Trust may also process personal information about staff where:

- Staff have given their consent;
- There is a need to protect someone's vital interests; or
- There is a legitimate interest in processing the personal data, for example to support the Trust to develop strategies and plans to support its sustainability.

7.3 Some of the reasons listed above for collecting and using personal information about staff overlap, and there may be several grounds that justify the Trust's use of staff personal data.

7.4 The Trust uses staff data to comply with legal obligations in relation to employment and the education of children in an Academy environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. The Trust will also use personal data when giving references.

7.5 The Trust considers that in some circumstances, the processing of personal data is necessary for its (or a third party's) legitimate interests, which include:

- Effective workforce management, including holiday entitlement, payroll matters, periodic performance reviews and, if required, disciplinary action;
- Ensuring that the information provided is accurate within the recruitment process and while staff are employed; and
- That it processes personal data to ensure staff have the right skills, training and experience for their role.

8.0 Other Individuals

8.1 The Trust may hold personal information in relation to other individuals who have contact with the Academies, such as volunteers and guests. Such information shall be held only in accordance with the GDPR principles, and shall not be kept longer than necessary.

9.0 Security of personal data

9.1 The Trust will take reasonable steps to ensure that members of staff will have access only to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR and DPA. The Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

9.2 For further details relating to security of IT systems, please refer to the E Safety Policy.

10.0 Sharing personal data

10.1 The Trust will not disclose personal data to a third party without consent unless it is satisfied that it is legally entitled to the data or it is required to provide the personal data by law. Where the Trust does disclose personal data to a third party, it will have regard to the data protection principles.

10.2 The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer or student;
- For the assessment of any tax or duty;
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract);
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- For the purpose of obtaining legal advice;
- To publish the results of public examinations or other achievements of students of the Trust;
- To disclose details of a student's medical condition where it is in the student's interests to do so, for example for medical advice, insurance purposes or to organisers of Academy trips;
- To provide information to another educational establishment to which a student is transferring;
- To provide information to the Examination Authority as part of the examination process; and
- To provide information to the Department for Education (DfE).

10.3 The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual students cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

10.4 The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about students, their parents or guardians, staff or other individuals. This information will not generally be disclosed except where:

- The Trust has the consent of the data subject;
- The law allows the Trust to disclose; or
- It is in the legitimate interests of the individual concerned or the Trust.

10.5 All requests for the disclosure of personal data must be sent to the Academy Principal, who will review and decide how to process, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure. Advice will be taken from the Data Protection Officer where necessary.

11.0 Confidentiality of student concerns

11.1 Where a student seeks to raise concerns confidentially with a member of staff, the Academy will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the Academy believes disclosure will be in the best interests of the student or other students.

12.0 Subject Access Requests

12.1 Anybody who makes a request to see any personal information held about them by the Trust will be making a subject access request. All information relating to the individual, including that held in electronic or manual files will be considered for disclosure.

12.2 All requests should be sent to the Academy Principal and must be dealt with in full without delay and at the latest within one calendar month of receipt.

12.3 Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 13, or over 13 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Academy Principal must, however, be satisfied that:

- The child or young person lacks sufficient understanding; and
- The request made on behalf of the child or young person is in the child or young person's interests.

12.4 Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Academy must have written evidence that the individual has authorised the person to make the application and the Academy Principal must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

12.5 Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

12.6 A subject access request may be made verbally or in writing. The Academy may ask for any further information reasonably required to locate the information.

12.7 An individual only has the automatic right to access information about themselves. The Trust will take care not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. The Trust will take particular care in the case of any complaint or dispute to ensure confidentiality is protected.

12.8 All files must be reviewed by the Academy Principal and Data Protection Officer before any disclosure takes place. Access will not be granted before this review has taken place.

12.9 Where all the data in a document cannot be disclosed a permanent copy will be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document will be retained, with the reason why the document was altered.

12.10 Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

12.11 There are other exemptions from the right of subject access. If the Trust intends to apply any of them to a request, then the Trust will explain which exemption is being applied and why.

13.0 Other rights of individuals

13.1 The GDPR sets out the rights of individuals under the law. Those rights are:

- The right to have data amended or corrected if it is inaccurate or incomplete;
- The right to have data erased in certain circumstances;
- The right to restrict processing in certain circumstances;
- The right to data portability in certain circumstances;
- The right to object to processing data in certain circumstances;
- Rights in relation to automated decision making and profiling;
- The right to withdraw consent;
- The right to lodge a complaint with a supervisory authority.

14.0 Right to object

14.1 Parents, carers, students aged 13 or over or staff can object to the processing of their personal data which is necessary for:

- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- The purposes of the legitimate interests pursued by the Trust or a third party, including profiling.

14.2 If the Trust receives such an objection to the processing as set out above, it will no longer process that personal data unless it can demonstrate:

- Compelling legitimate grounds for the processing which override the data subject's interests, rights and freedoms; or

- That the processing is required for the establishment, exercise or defence of legal claims.

14.3 Parents, carers, students aged 13 or over should submit their request to their Academy Principal in writing. Staff should contact the Director of Human Resources and Communications to make a request. Requests will be responded to within ten working days.

15.0 Right to rectification

15.1 An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, and where adequate evidence of inaccuracy is given, the data will be amended as soon as reasonably practicable, and the individual notified.

15.2 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal will be noted alongside the data, and communicated to the individual. The individual will be given the option of an appeal directly to the Information Commissioner.

15.3 An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way will be updated without undue delay.

16.0 Right to erasure

16.1 Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- Where consent is withdrawn and there is no other legal basis for the processing;
- An objection has been raised under the right to object, and found to be legitimate;
- Personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- Where there is a legal obligation on the Trust to delete.

16.2 The Chief Operating & Financial Officer and/or the Director of HR & Communications will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, or has been made public, reasonable attempts to inform those controllers of the request shall be made.

17.0 Right to restrict processing

17.1 The processing of an individual's personal data may be restricted:

- Where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;
- Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

- Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim; or
- Where there has been an objection made under para 14 above, pending the outcome of any decision.

18.0 Personal Data Breaches

18.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

18.2 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

18.3 Once notified, the Chief Operating & Financial Officer and/or the Director of HR & Communications must decide whether the breach meets the thresholds for reporting to the Information Commissioner's Office (ICO). The Trust must report the breach when, if not addressed in an appropriate and timely manner, it may result in:

- Physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights;
- Discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation;
- Damage to reputation;
- Loss of confidentiality of personal data protected by professional secrecy; or
- Any other significant economic or social disadvantage to the natural person concerned.

18.4 When reporting a breach, the Trust must provide:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Trust's Data Protection Officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and

- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

18.5 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust must inform those concerned directly and without undue delay. Information provided to those affected must include:

- The name and contact details of the Trust's Data Protection Officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, the measures taken to mitigate any possible adverse effects.

18.6 If the breach meets the thresholds for reporting, the Chief Operating Officer or the Data Protection Officer will do so within 72 hours of becoming aware of the breach.

18.7 The Chief Operating Officer will be responsible for instigating an investigation into the breach, including how it occurred, and whether it could have been prevented. The Executive Team will review any recommendations for further training or changes in procedure and will decide how they should be implemented.

19.0 CCTV

19.1 The Trust's Academies use Closed Circuit Television cameras for monitoring their premises and supporting student behavioural policies. There are visible signs showing that CCTV is in operation and images from this system are securely stored where only a limited number of authorised persons may have access to them. The Trust may be required to disclose CCTV images to authorised third parties, such as the police, to assist with crime prevention or at the behest of a court order.

20.0 Biometric data

20.1 Some Academies use biometric information to provide cashless catering, library lending or access to photocopiers. Where these systems are in place, Academies use information taken from fingerprints to identify service users. Academies need consent to use biometric information, which they will ask for when students and staff join the Academy. Where consent is not secured, Academies will provide other ways for students and staff to access these services.

21.0 Profiling and automated processing

21.1 The Trust may use profiling, which is an automated process to evaluate certain things about individuals. Examples of profiling include:

- Information used to set targets for students. The Trust uses software to understand how similar students might perform in future based on the performance of children with similar ability nationally. Teachers use the information to set challenging but realistic targets for students.
- The monitoring and analysis of emails sent and received using Academy email accounts and analysis of websites visited using

Academy computers. The Trust uses software to log information and to alert Academy staff about access to inappropriate websites or emails sent with inappropriate content.

22.0 Transferring data internationally

22.1 The Trust will not transfer personal data outside the European Economic Area (EEA) unless such transfer complies with the GDPR. This means the Trust cannot transfer any personal data outside the EEA unless:

- The EU Commission has decided that another country or international organisation ensures an adequate level of protection for personal data; or
- The transfer of personal data is subject to appropriate safeguards, which may include:
- Binding corporate rules; or
- Standard data protection clauses adopted by the EU Commission.
- One of the derogations in the GDPR applies (including if an individual explicitly consents to the proposed transfer).

22.2 The Trust currently transfers personal data outside the EEA as some personal data is stored on cloud systems, the servers for which are based outside the EEA.

23.0 Contact details

23.1 Any questions or concerns relating to this policy should be directed to Northern Education Trust's Data Protection Officer:

Jim Gaff
Northern Education Trust
Cobalt Business Exchange Central, Unit 5, Silver Fox Way, Cobalt Business Park
Newcastle upon Tyne
NE27 0QJ

public.enquiries@northerneducationtrust.org

+44 (0)191 594 5070

23.2 Individuals wanting to exercise their right to to lodge a complaint with a supervisory authority should contact:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 (national rate number)

Website: https://ico.org.uk/concerns/