



Data Protection Policy

Newbury Academy Trust

September 2017

1. Introduction

- 1.1. "Academy", "Academy Trust" all refer to Newbury Academy Trust, Love Lane, Newbury, Berkshire, RG14 2DU. School refers to one of the three schools within the Newbury Academy Trust, Trinity School, Love Lane, Newbury, Berkshire, RG14 2DU; Fir Tree School, Fir Tree Lane, Newbury, Berkshire, RG14 2RA; Speenhamland School, Pelican Lane, Newbury, Berkshire, RG14 1NU.
- 1.2. The term Governor refers to both Full Governing Body Trustees and Local Governing Body Governors.

2. Aims

- 2.1. The Trust processes Personal Data (as defined below) in order to enable it to provide education and other associated functions (and, additionally, where there is a legal requirement to process the personal data to ensure that it complies with its statutory obligations). This Data Protection Policy outlines the practices in place in relation to the handling of personal information to ensure that the Trust and its staff are acting in accordance with UK laws and regulatory guidance. The policy also describes individuals' rights in relation to their Personal Data processed by the Trust. These practices, together with this Policy and the Freedom of Information Policy ensure that all staff in the Trust fully understand the Trust's obligation to abide by the data privacy laws and regulations of the UK. The Trust and its staff is committed to complying with data protection legislation at all times.
- 2.2. The Data Protection Act stipulates that anyone processing personal data must comply with eight principles of good practice; these principles are legally enforceable. The principles require that personal information is:
 - processed fairly and lawfully;
 - obtained only for specified and lawful purposes;
 - adequate, relevant and not excessive in relation to the purposes for which it is processed;
 - accurate and where necessary, kept up to date;
 - not kept for longer than is necessary;
 - processed in accordance with the rights of individuals;
 - kept secure;
 - not transferred to a country or territory outside the EEA

3. Personal Data

- 3.1. Personal Data is any information (for example, a person's name) or combination of information about a living person which allows

that living person to be identified from that information (for example a first name and an address).

- 3.2. Examples of Personal Data which may be used by the Trust in its day to day activities include names, addresses (email and property addresses), telephone numbers and other contact details, educational records, CVs, photographs, performance reviews, payroll and salary information and images obtained through CCTV.
- 3.3. The laws governing how we can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word-processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets).
- 3.4. Data protection laws are enforced in the UK by the Information Commissioner's Office ("ICO"). The Trust maintains a notification with the ICO which sets out how it Processes Personal Data and for what purposes. Our notification can be viewed by visiting <https://ico.org.uk/ESDWebPages/DoSearch> and searching for
"Trinity School" or our registration number "Z3644790"
"Fir Tree School" or our registration number "Z3644790"
Speenhamland School or our registration number "Z8227259"

4. Acquiring and Processing (Using) Personal Data

- 4.1. The Trust processes Personal Data (including Sensitive Personal Data, see below for more information) of individuals including its staff, students, parents or carers, contractors, business contacts, customers, suppliers and any other individuals who come into contact with the Trust, including job applicants, former staff, prospective and former students, depending on the relationship with them, for a number of specific legitimate purposes. These are:
 - providing students and staff with a safe and secure environment, an education and pastoral care;
 - providing activities for students and parents - this includes school trips and activity clubs;
 - providing academic, examination and career references for students and staff;
 - protecting and promoting the interests and objectives of the Academy and the Trust – this includes fundraising;
 - fulfilling the Academy's and the Trust's contractual and other legal obligations.
- 4.2. Trust staff must not process Personal Data for any other purpose without the Executive Headteacher's permission.

- 4.3. We may share Personal Data with schools within the Trust. We may also share Personal Data with any third party service providers, such as in relation to our human resources information systems, or other service providers, which we appoint in the future to Process Personal Data on behalf of the Trust.

5. Fair and Lawful Use of Personal Data

- 5.1. One of the main data protection obligations requires the Trust (and its staff) to process Personal Data fairly and lawfully. In practice, this means that the Trust (and each staff member) must comply with at least one of the following conditions when Processing Personal Data:
- the individual to whom the Personal Data relates has consented to the Processing (unless under the age of 12 and not able to fully understand their rights in this regard, in which case consent should be sought from a parent or guardian)
 - the Processing is necessary for the performance of a contract between the Trust and the individual;
 - the Processing is necessary to comply with a legal obligation placed on the Trust; or
 - the Processing is necessary in order to pursue the legitimate interest of the Trust and is not unfair to the individual
- 5.2. The Trust has special obligations in connection with the use of Sensitive Personal Data, namely information about an individual's race, ethnic origin, political or religious beliefs, trade union membership, health, sex life and actual or alleged criminal activity.
- 5.3. The Trust does not generally seek to obtain Sensitive Personal Data unless:
- the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the Trust is collecting the data;
 - to monitor learners' attendance and the reasons for non-attendance;
 - the Trust needs to do so to meet its obligations or exercise its rights under employment law and/or pastoral duties on behalf of learners; or
 - in exceptional circumstances such as where the processing is necessary to prevent and/or detect crime or to protect the vital interests of the individual concerned (i.e. in "life or death" circumstances).
- 5.4. Sensitive Personal Data should not be emailed or disclosed unless measures are taken to encrypt or otherwise secure that

information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray.

- 5.5. The Trust shall not hold unnecessary Personal Data, but shall hold sufficient information for the purpose for which it is required. The Trust shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.
- 5.6. The Trust shall only keep Personal Data for as long as is reasonably necessary. More specific guidelines apply in particular situations: further details are available from the Trust Business Manager.
- 5.7. The Trust shall do all that is reasonable to ensure that Personal Data is not lost or damaged, or accessed or used without proper authority, and the Trust shall take appropriate steps to prevent these events happening. In particular:
 - paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended;
 - the Trust uses a range of measures to protect Personal Data stored on computers, including file encryption, anti-virus and security software, user passwords, audit trails and back-up systems;
 - staff must not remove Personal Data from the Academy's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the ICT Services Manager;
 - staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased;
 - staff must not use personal accounts for email and file sharing of Personal Data.
- 5.8. The Trust shall not transfer Personal Data outside the European Economic Area (EEA) without the Data Subject's permission unless it is satisfied that the Data Subject's rights under the Act will be adequately protected. This applies even if the transfer is to a student's parents or guardians living outside the EEA.

6. Information and explanation

- 6.1. Unless it is already clear to the person concerned, when the Trust asks for personal information which may be kept as Personal Data the Trust shall:

- explain which information is optional, which is mandatory, and the consequences if it is withheld;
- explain why the Trust is asking for that information, and how it will be used;
- identify the Trust as the data controller;
- explain who outside the Trust will receive that information.

See the Trust Privacy Statements (Appendix 1) for more information

6.2. If the Trust obtains personal information from someone other than the Data Subject, the Trust shall:

- inform the Data Subject that the Trust has recorded that information;
- identify its source;
- explain why the Trust has acquired it, and how it will be used;
- identify the Trust as the data controller;
- explain who outside the Trust will receive that information.

6.3. A different approach may be necessary when medical, child protection or staff issues are involved, further advice is available from the Executive Headteacher.

7. Protecting confidentiality

7.1. Only staff with the appropriate authorisation from the Trust may access any Personal Data. Personal Data shall not be disclosed to anyone who does not have the appropriate authority to receive such information. This is irrespective of their seniority within the Trust, their relationship to the Data Subject or their professional role (such as a Police Officer), unless they need to know it for a legitimate purpose and if required have the correctly authorised paperwork.

7.2. The Trust will not disclose anything on a pupil or student's record which would be likely to cause serious harm to their physical or mental health or that of anyone else.

7.3. Any information disclosed relating to Child Safeguarding issues are fully subject to the Trust's Child Protection Policy.

7.4. Where there is doubt or statutory requirements conflict advice should be obtained.

8. Requests for information

- 8.1. Individuals are entitled to know whether the Trust is holding any Personal Data which relates to them, what that information is, the source of the information, how the Trust uses it, and who it has been disclosed to.
- 8.2. Individuals have a legal right to ask the Trust not to use their Personal Data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.
- 8.3. Whether or not a photograph comes under the DPA is a matter of interpretation and quality of the photograph. However, the Trust takes the matter extremely seriously and seeks to obtain parents' permission for the use of photographs outside their home academy and the Trust. In particular, the Trust will record their wishes if they do not want photographs to be used of their children.
- 8.4. Individuals have a legal right to ask for incorrect Personal Data to be corrected or annotated.
- 8.5. Individuals have a legal right to ask the Trust not to make automatic decisions (using Personal Data) if such automatic decisions would affect them to a significant degree.
- 8.6. Any member of staff who receives a request for information covered by this policy from a student, parent or any other individual must inform the Executive Headteacher as soon as is reasonably possible, which should in most cases be the same day. This is important as there is a statutory procedure and timetable which the Academy must follow for Freedom of Information Access (FOIA) requests and Subject Access Requests (SARs).
(See the FOIA Policy)

9. Compliance with This Policy

- 9.1. The ICO can investigate complaints, audit the Trust's use or other Processing of Personal Data and can take action against the Trust (and you personally in some cases) for breach of these laws. Action may include making the Trust pay a fine and/or stopping the use by the Trust of the Personal Data, which may prevent the Trust from carrying on its educational and associated functions. Organisations who breach one or more laws on Personal Data also often receive negative publicity for

the breaches which affects the reputation of the Trust and its activities as a result.

- 9.2. Each Trust staff member or Third Party is required to read and comply at all times with this Policy. In this Policy, a "Third Party" is anyone who is not employed by the Trust, for example employees of other schools, agents, external organisations, consultants, contractors, and service providers.
- 9.3. A member of staff who deliberately or recklessly discloses Personal Data held by the Trust without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

| | |
|-------------------------------------|-------------------------------------|
| Authorised by | Resolution of the Board of Trustees |
| Date | 11 th October 2017 |
| Effective Date of the Policy | 12 th October 2017 |
| Effective Date for Review | 11 th October 2019 |