The Rose Learning Trust

TRANSFORMING FUTURES COLLABORATIVELY

THE ROSE LEARNING TRUST

DATA PROTECTION POLICY

Reviewed: **May 2017**

Next Review: **May 2018**

This document is a statement of the aims and principles of the Trust, for ensuring the confidentiality of personal data and sensitive personal data relating to staff, pupils, parents/carers and governors.

Introduction

The Rose Learning Trust and its academies need to keep personal data about its employees, students and other users to allow it to monitor performance, achievement, health and safety, t process data so that staff can be safely recruited and paid, to manage the professional development of staff and to discharge other functions associated with the provision of education. In addition, there may be legal requirement to collect and process personal data to ensure that the Trust and its academies comply with statutory obligations.

The Trust will publicise this Policy on the Trust website and copies will be available for all academies within the Trust.

For the purpose of this policy The Rose Learning Trust includes the Trust as well as each member academy.

The Rose Learning Trust recognises that in order to operate and meet its legal obligations it needs to collect and use personal data as defined by the Data Protection Act 1988. It also recognises that this personal information must be dealt with properly however it is collected, recorded and use – whether on paper, in a computer or recorded on other material – and there are safeguards to ensure this is in the Data Protection Act 1998.

The Rose Learning Trust regards the lawful and correct treatment of personal information as very important to successful operation, and recognises the need to maintain confidence between those with who it deals and the Trust. It also recognises the need to ensure that it treats personal information lawfully and correctly

Relationship to other Academy Policies

This Policy relates to all the Academy Policies which involve the collection and storage of information about people. There is also a separate publication schedule relating to Freedom of Information

Purpose

This policy is intended to ensure we collect information fairly, use it lawfully and keep it safe in order to comply with the Data Protection Act. This policy applies to any information we hold that relates to identifiable living persons.

The Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the Trust. We use this personal information to provide education and for functions associated with the running of our Trust.

We are registered as a data controller with the Information Commissioner's Office (ICO). Details of the information we hold and the purposes we use it for can be found on the ICO's online Data Protection Register at www.ico.org.uk.

All employees, directors, governors, contractors, agents, volunteers and temporary staff must work in accordance with this policy and associated guidance.

What was consulted?

The Policy was informed by the Information Commissioners Office official guidance for public sector organisations concerning Data Protection in education (www.ico.gov.uk)

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the academies from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller

The Rose Learning Trust (the Trust) as a body corporate is registered as a Data Controller with the Information Commissioners Office (ICO). Academies that are members of the Trust are also named in the registration as Data Controllers. As such, the Governors of each academy is responsible for ensuring the requirements of the Data Protection Act 1998 (DPA) are implemented at establishment level. However, the Designated Data Controllers at each Academy will deal with day to day matters.

The Rose Learning Trust also has 2 Designated Data Controllers. These are the Chief Executive Officer and the Chief Operations Officer

The Data Protection Principles

The Data Protection Act contains 8 principles that we must comply with:

- Personal data shall be processed fairly and lawfully;
- Personal data shall be obtained only for one or more specified and lawful purposes;
- Personal data shall be adequate, relevant and not excessive;
- Personal data shall be accurate and where necessary, kept up to date;
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act;
- Appropriate policies, procedures and technical measures will be put in place to protect personal information;
- Personal data shall not be transferred outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

Unless there is an exemption within the Data Protection Act or other legislation we will do the following in order to comply with the 8 principles:

- explain why we are collecting information and how it will be used at the point we first collect it;
- share information with others only when it is lawful to do so and, whenever possible, with the consent of the person(s) it relates to;
- take extra care in our processing of sensitive personal data which includes information about physical or mental health, religion, race and criminal convictions and proceedings;
- avoid using personal information for any new or substantially changed purposes which were not explained at the point the information was first collected;
- check the quality and the accuracy of the personal information we hold and act quickly to correct details that are found to be inaccurate;
- ensure information is not retained for longer than is necessary;
- ensure that we dispose of information which is no longer required in a safe and secure manner;
- ensure that appropriate safeguards are in place to protect personal information from loss, theft, damage, unauthorised access, unauthorised disclosure or unplanned destruction;
- ensure we have effective procedures to deal with requests from anyone who asks for a copy of the information we hold about them;
- ensure our staff understand our policies and procedures and are provided with appropriate data protection training;
- confirm the identity of persons who contact us before we disclose any personal information to them;

- use appropriate methods to send personal information to third parties in order to ensure it safely reaches the destination;
- investigate any known or suspected information security breaches and take steps to address any risks which are identified;
- obtain assurances from our suppliers and contractors on their data protection and information security standards before allowing them to access the personal information we hold.

Compliance

All staff directors and governors must work in accordance with this policy and associated guidance. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Trust. Any failures to follow the policy can therefore result in disciplinary procedure. which may lead to dismissal.

Staff must remember that they can be prosecuted for breaching the Data Protection Act. Under the Act offences include accessing, obtaining or disclosing information without the data controller's permission and selling, or offering to sell, personal information which has been obtained illegally.

Responsibilities of Staff

All staff are responsible for: -

Checking that any information that they provide to the Trust/academy in connection with their employment is accurate and up to date.

Informing the Trust/academy of any changes to information that they have provided e.g. change of address, either at the time of appointment or subsequently.

The Trust cannot be held responsible for any errors unless the staff member has informed the Trust/academy of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a pupil's work, opinion about ability, references to other academic institutions or details of personal circumstances), they must comply with the guidelines for staff set out in the Staff Code of Conduct.

Data Security

All staff are responsible for ensuring that: -

- Any personal data that they hold is kept securely
- Personal information is not disclosed either orally or in writing or via Web pages or by other means, accidentally or otherwise, to any unauthorised third party

Staff should note that unauthorised disclosures will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Kept in a locked filing cabinet, drawer, safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network that is regularly backed up; and
- If a copy is kept on a removable storage media, that media must be encrypted with bit locker or similar software
- If required to be transmitted by email, be encrypted using Trust approved encryption methods

Complaints

Complaints and concerns relating to our use of personal information will be taken seriously and will be dealt with in accordance with our complaints policy. Where the complainant is not satisfied with the outcome they may contact the Information Commissioner's Office.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk, telephone 0303 123 1113 (local rate) or 01625 545745 (national rate)

Review

This policy will be reviewed at least every 2 years. The review will be undertaken by the Headteachers, or their nominated representative. The guidance which supports this policy will be updated as required and will be communicated to all staff, directors, governors and any other relevant persons with access to personal data held by the Trust

Contact

If you have any enquires in relation to this policy, please contact the School Business Manager of the issuing school who will also act as the contact point for any requests for personal and educational information held by the trust.

Appendices

Appendix 1 – Subject Access Requests

Appendix 2 – Requests for Access to Pupil Records & School Reports

Appendix 1

Rights of access to information

Any person can request access to their personal information which is held by the trust in accordance with the Data Protection Act. This is known as a Subject Access request or SAR. There is a separate process for accessing a pupil's educational record in accordance with the Education (Pupil Information) (England) Regulations 2005, please refer to Appendix 2.

Subject Access Requests

All staff, parents and other users are entitled to:-

- Know what information the Trust holds and processes about them or their child and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the Trust is doing to comply with its obligations under the 1988 Act

Requests for information must be made in writing (this can include email).

Requests will be answered within 40 calendar days however this period will not begin, or may be suspended, until:

- the identity of the applicant has been clearly established (the trust reserves the right to request sight of identity documents such as passport or driving licence);
- any clarification the trust requests on what information is required is provided by the applicant;
- payment of any fee, the Data Protection Act permits the trust to charge £10 for each request.

Any individual may request access to information held about them. However, for children this depends upon their capacity to understand and to take informed decisions about themselves (normally from around the age of 12). The Headteacher or their representative will discuss any request involving a child's records with the child and take their views into account when making a decision on whether information should be disclosed.

A child with competency to understand can refuse to allow a request for their records, even if it is made by their parent or guardian. Where the child is not deemed to be competent an individual with parental responsibility or their guardian shall make the decision on behalf of the child.

Complaints

Complaints about Subject Access Requests should be made to the Chairperson of the trust board who will decide whether the complaint may be dealt with in accordance with the trust's complaints procedure. Complaints that cannot be dealt with through the trust's complaints procedure can be considered by the Information Commissioner's Office. We will include details of how to complain where we respond to SARs.

Appendix 2

Education (Pupil Information) (England) Regulations 2005

The Regulations

Under these regulations, the governing body of a trust must make a pupil's educational record available for inspection by the parent, free of charge, within 15 school days of the parent's written request for access to that record.

The trust must also provide a copy of the record if requested to do so in writing within 15 school days. The trust may charge a fee not exceeding the cost of supply.

The meaning of parent is wider than the definition of who has parental responsibility. Parent means a person with parental responsibility or who has care of the child. Therefore, where a child is living with grandparents, the grandparents have a right to see the child's educational record even though they may not have parental responsibility which would allow them, for example, to change the child's name.

Parents have a right to access their child's data under the Pupil Information Regulations and the child cannot prevent this. These Regulations only cover information in the official pupil record.

Exemptions

A trust must not communicate anything to the parent which it could not communicate to the pupil under the DPA. Also, the trust must be mindful of other individuals' rights under the DPA which might be infringed. For example, where a pupil's parents have divorced and the record contains letters from the pupil's mother, consideration must be given to whether these should be removed from the record before it is shared with the father.

School reports

Every parent is entitled to receive an annual report in respect of his or her child. Parents also have the right to make arrangements to discuss the content of the report with the child's teacher. This right remains even if a child no longer lives with the parent, providing that parent has parental responsibility.