



Information Access and Governance Policy

This policy encompasses the Data Protection Policy

Policy Monitoring, Evaluation and Review

This policy is effective for all academies within the Rushey Mead Educational Trust, the Teaching School, the SCITT and all other activities under the control of the Trust and reporting to the Trust Board.

Version:	5.0
Date created:	July 2017
Author:	P Ticher
Ratified by:	Board of Trustees
Date ratified:	3 rd October 2017
Review date:	January 2018

Revision History:

Version	Date	Author	Summary of Changes:
1.0	04.06.2015	PTI/SCA	Update of policy.
2.0	13.08.2015	CRO	Amendment of policy to reflect conversion to academy status.
3.0	12.01.2016	SGR	Update as a result of amendment to FOI Act
4.0	08.06.2016	CJO	Insertion of text relating to requests of information relating to Leicester City Council
5.0	July 2017	CJO	Removal of Freedom of Information Policy.

Summary

Rushey Mead Educational Trust ensures that it gives all data subjects the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and information about the individuals' rights of access.

The data held is adequate, relevant, accurate and up to date (where necessary), and is not excessive or held longer than necessary.

Confidential information (electronic or otherwise) is kept secure at all times, and additional security precautions are applied when it is taken off site.

Information about the Rushey Mead's Data Protection Policy is available from the front office of the respective academy and can also be viewed on the Academy's website.

Information is also available about how to make a Subject Access Request and how to apply to the academy for a student's educational records.

Full policy

Contents

Scope.....	1
Responsibilities.....	1
Confidentiality and information sharing	2
Data Protection.....	3
Security measures.....	4
Access to Information.....	5
Monitoring.....	6
Appendix 1: Rushey Mead Educational Trust.....	7
Subject Access Request Form.....	7

Scope

This policy describes how Rushey Mead Educational Trust protect the confidential information they hold, provide access to information where appropriate and comply with relevant provisions of the following legislation (referred to as 'the legislation' in this policy):

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005

In particular this policy covers the information held about students and their families, but it also applies to information about staff and other individuals, and about the workings of the Trust.

Responsibilities

Rushey Mead Educational Trust has overall responsibility for compliance with the legislation.

The Data Protection Officer (DPO) is the Chief Operating Officer. The DPO also oversees compliance with Freedom of Information requests and requests for educational records.

Day to day compliance with all aspects of the legislation is delegated to the Principal.

All staff that handle data covered by the legislation or by confidentiality have a responsibility to understand their obligations and, in particular, to inform the DPO immediately if they are aware of any adverse event that is serious or that cannot be immediately rectified, and of any 'near misses' that indicate areas where current practice could be improved.

A deliberate breach of this policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

The DPO is responsible for:

- ensuring that all procedures for handling data and holding it securely are designed to support compliance with the legislation.
- ensuring that all staff and governors receive appropriate induction and training on the legislation and their responsibilities for confidentiality.
- authorising non-routine disclosures of data.
- ensuring that all contracts with data processors are compliant with the Data Protection Act requirements.
- notification of data processing activities to the Information Commissioner in the form required by the legislation.

Confidentiality and information sharing

Most of the information held by the Trust about individuals is confidential. This does not mean that it is secret, but that it is shared only on a “need to know” basis and in accordance with legal requirements. When confidential personal data is treated on this basis this is consistent with the relevant parts of the Data Protection Act.

All those who have access to confidential information should take particular care not to breach confidentiality inadvertently, for example through:

- Discussing confidential information with family and friends, especially if this allows individuals to be identified.
- Talking about confidential information where it can be overheard.
- Working on confidential information in places where it might be seen.
- Sharing information without checking whether it is confidential – in particular where there are issues within a family.

Information about students

When data on students is shared, whether within or outside the Trust, the interests of the student must remain paramount. Students should normally be **aware** of the extent of data sharing. In non-routine situations they should, whenever possible, be **consulted** and their wishes taken into account. The exceptions to this are:

- When there is an over-riding reason for sharing information without the consent and/or knowledge of the student, e.g. child protection
- When the student does not have the capacity to make a competent decision concerning the sharing of information about them. In such instances, those who are responsible for the student should be consulted.

Students should be made aware that absolute confidentiality cannot be guaranteed if the student’s own safety or the safety of others is at risk.

Sharing data within the Trust

The normal running of an Academy requires considerable amounts of information to be shared routinely between staff and with parents/carers about students’ activities and educational performance.

Information that is more confidential – for example about the student’s personal issues or family situation – may be shared for legitimate reasons such as:

- for information (e.g. to ensure others may respond appropriately in the case of classroom management or potential problems);
- for the clear benefit of the student;
- because action is required (e.g. to inform the Designated Senior Person in the case of possible Child Protection issues).

Sharing data with parents/carers

Parents/carers have a right to their child's educational records; information about the student's activities and educational performance may be shared with parents/carers as a matter of course.

More confidential information should not be shared with parents/carers unless the student has been informed and their views taken into account, to the extent possible given the student's age and capacity.

Sharing or disclosing data outside the Trust

The student's consent is not required for disclosure of student data to authorised recipients where the disclosure is required by law.

Where an information sharing agreement is in place to cover routine information sharing the provisions of the agreement must be complied with.

Confidential data should be shared externally in other cases only for over-riding reasons (such as child protection). It must be shared only by a trained and authorised person and to the appropriate authorities. Any other person who believes that a disclosure might be necessary must consult the DPO or another appropriately trained member of staff.

Disclosures to third party contractors may be made only where an appropriate contract is in place to underpin their obligation of confidentiality.

Disclosure of information about staff

Personal data about staff will normally be released to third parties only with the individual's knowledge and almost always with their consent (ideally in writing).

Requests for disclosure from an external body will not be accepted unless they are in writing on headed paper and give full reasons.

Requests for disclosure without consent must be for specific over-riding reasons such as prevention or detection of crime, the health, safety and welfare of other employees or students, or where disclosure is to protect the vital interests of the individual. Any such disclosure must be authorised by the DPO.

Whenever data is disclosed, the staff member should be informed even if their consent has not been sought, unless the agency to which the data is disclosed advises officially that the individual not be informed.

Data Protection

The Data Protection Act:

- Regulates the processing of personal data relating to living individuals (Data Subjects)
- Imposes legal obligations upon data controllers (the academy)
- Provides Data Subjects with legal rights including the right to know what data about them is being processed
- Introduces sanctions for breaches of the Act

The Act applies to 'personal data'— essentially any recorded information about identifiable individuals. (Confidentiality can apply both to recorded information and to information that is not recorded anywhere, such as conversations or actions that have been observed.) Personal data therefore includes, but is not limited to:

- Most academy records about students
- Most academy records about staff

Rushey Mead Educational Trust aims to fulfil its legal obligations by ensuring that in processing personal data it complies with the eight Data Protection Principles that are fundamental to the Act.

Transparency & Choice (Data Protection Principles 1 & 2)

Personal data will not normally be used without the individual's knowledge. Individuals should also be made aware of any non-obvious purposes for which it might be used and any non-obvious disclosures that might be made to outside bodies.

All staff who collect data from individuals (students, parents/carers, staff or others) should normally use school-approved forms (electronic or paper) that comply with the above requirements. If in any doubt, forms should be checked with the DPO before being used.

Where data may be used in ways that are not essential to the running of the academy individuals will, where practicable, be given the opportunity to opt out of this use.

Data quality (Data Protection Principles 3 & 4)

In order to ensure that data is adequate, relevant and not excessive in relation to the purpose for which it is being held, each academy should check records regularly for missing, irrelevant or seemingly excessive information.

In order for data to be as accurate and as up-to-date as is reasonably possible, records must be updated as soon as practicable if anyone informs the Academy of a change of any of their details. Data generated within the school must be recorded in accordance with good record-keeping practice and in line with the school's guidance on student data.

Annually, parents/carers and staff are asked to update the contact information held by the academy for accuracy. Also, admin staff should check any information held by the academy against parental consent forms for trips.

If a data subject challenges the accuracy of their data, the school must immediately mark the record as potentially inaccurate. If the disagreement cannot be resolved informally it will be referred to the Governing Body for their judgement. Until resolved the marker will remain and all disclosures of the affected information will contain both versions of the information.

Data retention (Data Protection Principle 5)

Data held about individuals must not be kept longer than necessary. Relevant staff must ensure that obsolete data is properly erased at the right time, in accordance with the Academy's Retention Schedule.

CCTV & monitoring

The Academies use CCTV where appropriate, and place prominent notices to inform anyone who enters their premises. Use of CCTV complies with guidance issued by the Information Commissioner.

Rushey Mead Educational Trust's academies reserve the right to monitor computer use, for the purposes of improving system performance, preventing and detecting intrusion or attempted intrusion, identifying breaches of policy on acceptable use and preventing or detecting malicious or fraudulent use. Such monitoring will be proportionate and carried out with the minimum impact on personal privacy. Investigation of the behaviour of specific individuals will take place only where there is an established cause for concern and with authorisation from the Principal or member of the Senior Leadership Team.

Security measures

Each Rushey Mead Educational Trust academy has procedures in place to ensure appropriate use, disclosure and protection of personal data. Each academy should use – and train its staff in the use of – physical and electronic safeguards to ensure the security of data. These include, but are not limited to:

- Locks to filing cabinets
- Locks to doors, to offices, filing rooms and computer rooms
- Secure management of the holding and storage of keys
- Access control to buildings where confidential information may be held, and particularly to areas holding significant amounts of personal data.
- Anti-virus software installed

- Firewall software/hardware installed
- Reliable data backup and recovery procedures
- Procedures for authorising access to appropriate data, and for issuing and revoking log-on credential
- Good practice relating to passwords, clear screens, locking of computers
- Separate computer areas for administration and teaching
- Clear desk/clear screen procedures when work areas are unattended.
- Procedures for sending confidential information both electronically and by mail
- Procedures for authorising staff only when strictly necessary to take confidential data, both electronic and on paper, off the school premises or to access it outside the school premises.
- Procedures for ensuring that staff apply authorised security measures if they wish to use their personal devices of any kind (including memory sticks, smartphones, tablets, laptops and cameras) for storing confidential school-related data.
- Procedures for authorising the use of any cloud-based services, whether on the academy's account or on a personal account.

Access to Information

With regard to students, there are two distinct rights to information held by the academy:

1. **The subject access right** – where a student has the right to a copy of their own information. In certain circumstances – and generally while the child is under 12 – requests may be made by a parent/carer on behalf of their child.
2. **Rights to the educational record** – under the Education (Pupil Information) (England) Regulations 2005, a parent/carer has the right to access their child's educational record.

All requests should be addressed to Rushey Mead Educational Trust in writing. The DPO will ensure that the request is responded to appropriately within the legal time limit – subject access: 40 calendar days; educational records: 15 school days.

The response to Subject Access Requests from students will be given directly to the student, unless it is clear that the student does not understand the nature of the request. Requests from students who do not appear to understand the nature of the request will be referred to their parents/carers or carers.

Requests from parents/carers in respect of their own child's educational records will be processed under the Education (Pupil Information) Regulations. Requests from parents/carers for other information about their child will, if appropriate, be treated as Subject Access Requests on behalf of the data subject (the child), provided the parents' bona fides can be satisfactorily established. The response will be sent in a sealed envelope to the requesting parent/carers.

Before responding, the DPO will apply any necessary and permitted exemptions, redactions, or decisions to withhold data. This can include cases where the information might cause serious harm to the physical or mental health of the students or another individual, where it would infringe a third party's confidentiality, or the request would entail releasing examination marks before they are officially announced.

Straightforward requests for information are normally provided free of charge. More complex Subject Access Requests are charged the permitted maximum (currently £10) and the enquirer notified of the charge at the time the request is submitted. (Note that the 40-day time limit starts once the fee has been received.)

A record of each access request will be kept, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), the date of supplying the information and the date and nature of any intermediate steps taken (such as verifying identity).

Monitoring

As far as possible, Rushey Mead Educational Trust uses automated systems to block access to inappropriate web sites or to filter out unacceptable e-mails, in order to avoid breaching users' privacy.

Users should be aware that no e-mail sent or received, and no web session, can be considered totally private. All activity on the system, including file deletion, leaves an audit trail and may potentially be recovered.

E-mail traffic and web sites accessed are routinely monitored.

Where there is apparent excessive use of the internet for personal reasons, access to inappropriate web sites or any other apparent breach of the acceptable use policy, Rushey Mead Educational Trust reserves the right to investigate further. This investigation may involve more detailed monitoring of the content of the user's internet use, including material identified as personal if this is appropriate in all the circumstances. An appropriate senior member of staff will authorise a qualified person to carry out such investigation, who must be satisfied that the case for investigation has been made, and that the type of investigation being proposed is proportionate to the apparent breach of policy.

Users will normally be informed that they are being investigated or monitored. In exceptional cases covert monitoring will be authorised where it is the only reasonable way of obtaining evidence of criminal activity or continuing gross misconduct, and it is necessary to avoid alerting the user.

E-mails and files held under the name of a member of staff may be accessed when they are away from the academy for any reason if it is necessary for the business of the academy. This action will only be authorised by the Principal, Executive Principal or Business Manager at the request of the absent staff member's colleagues, and where the absence is either unplanned, likely to be lengthy, or in an emergency.

When access is obtained for this purpose, care will be taken not to open or read any e-mail or other file which is clearly personal.

Wherever possible, members of staff planning to be absent should make their own arrangements for work-related e-mails and files to be accessible to colleagues.

Appendix 1: Rushey Mead Educational Trust

Subject Access Request Form

Date received: _____

RUSHEY MEAD EDUCATIONAL TRUST

Subject Access request (Data Protection Act 1998)

Any individual (a 'Data Subject') is entitled to see most of the information we hold about them. Where a child is unable to make their own application a parent/carer may apply on their behalf. Note that parents/carers also have the right to apply directly for their child's education record.

If you want to apply under the Data Protection Act, please fill in this form and hand it in to the office, with the £10 fee.

Your name: _____

Your address: _____

A phone number where we can contact you (if you wish): _____

Name of the Academy request pertains to: _____

Name of the Data Subject if different from the person applying: _____

Is or was the Data Subject:

A student

A parent/carer

A member of staff

If they are no longer associated with the academy, when was their last contact? _____

If you have not ticked any of the above, please tell us of any reason why you think we might have information about this Data Subject: _____

If we may have known the Data Subject under a different name, please tell us here what it was:

If you are only interested in particular information, please say what that is:

I want to see the records you hold on me, and I enclose £10. Signature: _____

Please note:

- If the address you give above does not match the one in our records, we may have to ask you for additional identification.
- If you are not the Data Subject (the person the information is about), we will need evidence that you are authorised to act for the Subject.
- We will reply as quickly as we can, but we may take up to 40 days. If you have asked for a copy of the information, we will send it to the address you have given above.
- We have information about students, their parents/carers, school staff and certain other people. We don't keep this information once we no longer need it, so if you were in touch with us some time ago we may no longer have any information about you.

We will provide everything we have about you, except that we may be allowed to hold back information which is also about, or which identifies, someone else.