DATA PROTECTION & INFORMATION GOVERNANCE POLICY

Summary	Data Protection and Information Governance Policy
Responsible Person/Author:	Adam Marham - COO
Applies to: (please circle/delete as appropriate)	**Staff ☒** **Student☒** **Community ☒**
Ratifying Committee(s) and Date of Final Approval:	Trust Board
Available On:	Trust and Academy websites. SharePoint and on demand
Effective from:	30 August 2024
Date of Next Formal Review:	August 2025
Review Period	Annual
Status	Statutory
Owner	RMAT
Version:	3

DOCUMENT CONTROL

Date	Version	Action	Amendments
1	1	Policy created	Policy amended from previous Data Protection Policy
03.08.22	2	Policy amended	Provision of what the Trust will consider to be manifestly excessive in a Subject Access Request. Clarity of what the Trust expects from requests from the Police.
26.07.24	3	Policy amended	Nomenclature changed. Document changed throughout following solicitors' advice

Contents

Introduction

1. This policy is to ensure the RMAT complies with the requirements of the UK General Data Protection Regulation ("GDPR") as brought into force under the Data Protection Act 2018, the Environmental Information Regulations 2004 ("EIR") and the Freedom of Information Act 2000 ("FOIA") (together 'Data Protection Legislation'), associated guidance and Codes of Practice issued under the legislation. The policy is to be applied to the way RMAT collects, processes, holds, and shares personal data and recognises the need to treat it in an appropriate and lawful manner.

Data protection definitions

Term	Definition
Biometric Data	is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting
Biometric Recognition System	is a system that operates automatically (electronically) and: • Obtains or records information about a person's physical or behavioural characteristics or features; and • Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system
Data	is information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes students, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes

Term	Definition
Data Users	are those in RMAT whose work involves processing personal data. Data users must protect the data they manage in accordance with this data protection and information governance policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, sexual orientation or genetic or Biometric Data

Policy Statement

2. Everyone has rights with regard to the way in which their personal data is managed. During the course of our activities as an academy trust, we will collect, store and process personal data about our students, workforce, parents, and others. This makes us a data controller in relation to that personal data.

3. We are committed to the protection of all personal data and special category personal data for which we are the data controller.

4. The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

5. All members of staff must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action

6. Where members of staff have a specific responsibility in connection with Processing, such as capturing consent, reporting a Personal Data Breach, or conducting a Data Protection Impact Assessment as referred to in this Data Protection Policy or otherwise, then they must comply with the related policies and privacy guidelines.

About this policy

7. The types of personal data that we may be required to manage include information about students, parents, staff, and others that we deal with.

8. This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

9. This policy does not form part of any employee's contract of employment and may be amended at any time.

10. This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

Scope and Purpose of this Policy, who and what it applies to

11. Staff should apply this policy and associated policies and procedures mentioned in Appendix 1 and participate in all training if requested to do so by RMAT.

12. If a member of Trust staff considers that aspects of this policy have not been followed, this should be raised with the Academy Principal or the Data Protection Officer ("DPO").

13. This policy applies to all Members, Trustees, Local Review Board ("LRB") members and RMAT staff.

14. This policy applies to all students, parents, staff, and Directors of Southway and has been approved by the Directors of Rodillian at Southway Limited which operates Southway and references in this document to the Trust should be read as if Southway was an Academy in RMAT.

15. This policy applies to information in all forms including but not limited to:

- Hard copy of 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 stored on portable computing devices including mobile phones, tablets, cameras, and laptops;
- Speech, voice recordings and verbal communications including voicemail;
- Published web content, e.g. Intranet and Internet;
- Photographs and other digital images.

Data Protection Officer

16. As a Trust, we are required to appoint a Data Protection Officer (DPO). Our DPO is Adam Marham, and he can be contacted at amarham@rmat.uk or dpo@rmat.uk

17. The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

18. The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

Data Protection Principles

19. Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

- Processed fairly and lawfully and transparently in relation to the data subject;
- Processed for specified, lawful purposes and in a way which is compatible with those purposes;
- Adequate, relevant, and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and
- Processed securely using appropriate technical and organisational measures.

20. Personal Data must also:

- be processed in line with data subjects' rights;
- not be transferred to people or organisations situated in other countries without adequate protection.

21. We will comply with these principles in relation to any processing of personal data by RMAT.

Fair and Lawful Processing

22. Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

23. For personal data to be processed fairly, data subjects must be made aware:

- that the personal data is being processed;
- why the personal data is being processed;
- what the lawful basis is for that processing (see below);
- whether the personal data will be shared, and if so with whom;

- the period for which the personal data will be held;
- the existence of the data subject's rights in relation to the processing of that personal data; and
- the right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

24. We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any processing.

25. For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

- where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;
- where the processing is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);
- where the law otherwise allows us to process the personal data, or we are conducting a task in the public interest;
- where we are pursuing legitimate interests, (or these are being pursued by a third party), for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of data subjects; and
- where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

26. When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

- where the processing is necessary for employment law purposes, for example in relation to sickness absence;
- where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
- where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

27. We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter unless we have already provided this information such as at the time when a student joins us.

28. If any data user is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

Vital Interests

29. There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in extremely specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

30. Where none of the other bases for processing set out above apply then the Academy must seek the consent of the data subject before processing any personal data for any purpose.

31. There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

32. When students or Staff join RMAT, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

33. In relation to all students under the age of 12 years old we will seek consent from an individual with parental responsibility for that student.

34. We will seek consent directly from a student who has reached the age of 12, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

35. If consent is required for any other processing of personal data of any data subject then the form of this consent must:

    - Inform the data subject of exactly what we intend to do with their personal data;
    - Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
    - Inform the data subject of how they can withdraw their consent.
    - Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

36. Consent may need to be refreshed where we may need to process the Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first considered the consent.

37. The DPO must always be consulted in relation to any form of consent form before consent is obtained.

38. A record must always be kept of any consent, including how it was obtained and when.

Processing for limited purposes

39. In the course of our activities as a Trust, we may collect and process personal data. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other schools, parents, other students, or members of our staff).

40. We will only process personal data for any purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

Notifying data subjects

41. If we collect personal data directly from data subjects, we will inform them about:

- our identity and contact details as Data Controller and those of the DPO;
- the purpose or purposes and legal basis for which we intend to process that personal data;
- the types of third parties, if any, with which we will share or to which we will disclose that personal data;
- whether the personal data will be transferred outside the United Kingdom and if so the safeguards in place;
- the period for which their personal data will be stored, by reference to our Records Management Policy;
- the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and
- the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

42. Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible, thereafter, informing them of where the personal data was obtained from.

Adequate, relevant, and non-excessive processing

43. We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by Data Protection Legislation.

Accurate data

44. We will ensure that personal data we hold is accurate and kept up to date.

45. We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

46. Data subjects have a right to have any inaccurate personal data rectified. See further below in relation to the exercise of this right.

Timely processing

47. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.

48. We will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that the data be to be kept for a minimum time.

49. We shall seek to comply with the rights exercised by data subjects as set out in the section below relating to processing in line with data subjects' rights as soon as possible and within legal time limits. However, there may be instances where due to circumstances outside of RMATs control this may not be possible e.g. where the Academy or RMAT has been closed or is only partially operable. In such circumstances data subjects till be notified and provided details about the reason for the delay and when a response can be expected.

Processing in line with data subjects' rights

50. We will process all personal data in line with data subjects' rights, in particular their right to:

- request access to any personal data we hold about them;
- object to the processing of their personal data, including the right to object to direct marketing;
- have inaccurate or incomplete personal data about them rectified;
- restrict processing of their personal data;
- have personal data we hold about them erased
- have their personal data transferred; and

- object to the making of decisions about them by automated means.

The Right of Access to Personal Data

51. Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with RMATs Subject Access Request Procedure.

The Right to Object

52. In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task conducted in the public interest.

53. An objection to processing does not have to be complied with where RMAT can demonstrate compelling legitimate grounds which override the rights of the data subject.

54. Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

55. In respect of direct marketing any objection to processing must be complied with.

56. RMAT is not obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

The Right to Rectification

57. If a data subject informs RMAT that personal data held about them by RMAT is inaccurate or incomplete then we will consider that request and provide a response within one month.

58. If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the data subject within one month of their request that this is the case.

59. We may determine that any changes proposed by the data subject should not be made. If this is the case then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

60. Data subjects have a right to "block" or suppress the processing of personal data. This means that RMAT can continue to hold the personal data but not do anything else with it.

61. RMAT must restrict the processing of personal data:

- Where it is in the process of considering a request for personal data to be rectified (see above);

- Where RMAT is in the process of considering an objection to processing by a data subject;

- Where the processing is unlawful, but the data subject has asked RMAT not to delete the personal data; and

- Where RMAT no longer needs the personal data, but the data subject has asked RMAT not to delete the personal data because they need it in relation to a legal claim, including any potential claim against RMAT.

62. If RMAT has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction unless this proves impossible or involves a disproportionate effort.

63. The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

64. Data subjects have a right to have personal data about them held by RMAT erased only in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was originally collected;

- When a data subject withdraws consent – which will apply only where RMAT is relying on the individual's consent to the processing in the first place;

- When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object;

- Where the processing of the personal data is otherwise unlawful; and

- When it is necessary to erase the personal data to comply with a legal obligation.

65. RMAT is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- To exercise the right of freedom of expression or information;

- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

- For public health purposes in the public interest;

- For archiving purposes in the public interest, research, or statistical purposes; or

- In relation to a legal claim.

66. If RMAT has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure unless this proves impossible or involves a disproportionate effort.

67. The DPO must be consulted in relation to requests under this right.

The Right to Data Portability

68. In limited circumstances a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to another organisation.

69. If such a request is made then the DPO must be consulted.

The Right to be Informed

70. A Privacy Notice is available to individuals to provide information on the processing of their personal data. This is written in clear, plain language, which is concise, transparent, and easily accessible. The Privacy Notice that is provided to students aged 12 and over is written in a clear, plain manner that the student will understand. Privacy Notices detail all information that is required to be provided to data subjects under data protection law.

71. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any consequences of failing to provide the personal data, will be provided. This information will be supplied at the time the data is obtained.

72. Where data is not obtained directly from the data subject, information regarding the categories of personal data that RMAT holds, the source that the personal data originates from and whether it came from publicly accessible sources will be provided. This information will be supplied:

    - if disclosure to another recipient is envisaged, at the latest, before the data is disclosed and

    - if the data is to be used to communicate with the individual, at the latest, when the first communication takes place.

73. In order to efficiently fulfil RMATs duty of education provision it is sometimes necessary for RMAT to share information with third parties. Routine and regular information sharing arrangements will be documented in RMATs Privacy notices. Any ad hoc sharing arrangements will be conducted in accordance with data protection obligations.

74. We will not inform data subjects of information sharing where we are not legally required to do so, for example where personal data is shared with the Police. In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy in relation to the same.

The right to access

75. Individuals have the right to obtain confirmation that their data is being processed. Individuals have the right to submit a Subject Access Request ("SAR") to gain access to their personal data.

76. Requests should be made to the DPO.

77. Staff at each Academy should forward any SAR's, to the DPO within 24 hours of receipt. If any SARs are received from parents or carers regarding students who are 12 or over, the DPO will seek, and record, the consent of the student before releasing the information.

78. RMAT is required to verify the identity of the person making the request before any information is supplied. Requests are considered in line with data subject's legal rights and RMATs legal obligations. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

79. When RMAT receives an SAR, it will consider whether the request is proportionate and reasonable or manifestly excessive and unfounded. On considering the same RMAT will consider the following factors (this list is not exhaustive, and every case will be considered on its own): -

- Proportionality of the SAR v the costs of responding;
- The nature of the information requested;
- The context of the request and the relationship between RMAT and the requester;
- Whether refusing the request or acknowledging the holding of information may cause damage to the requester;
- Resources available to RMAT to respond to the request;
- Whether the request is repetitive of previous requests and whether a reasonable amount of time has not elapsed since the previous request;
- Whether it overlaps with previous requests

80. In considering whether sufficient time has elapsed in respect of a repeated request, the Trust will consider whether a reasonable interval has elapsed with reference to:

- The nature of the data and its sensitivity
- How often if at all the data has been altered.
- If the data has been deleted since the last request.
- Whether a further request is made before an earlier request has been responded to which repeats all or part of the first request
- Whether the information has already been provided to a requester under an alternative statutory disclosure mechanism such as the criminal justice system.

81. Where the request is manifestly unfounded or excessive, RMAT holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

82. Where RMAT believes a request is manifestly unfounded or excessive, it may choose to respond to the request subject to the requester making payment of a fee. RMAT will write to the requester explaining this indicating the time limit for responding to the request will not begin to run until such time as the fee is paid.

83. In determining the fee to be charged, RMAT will take into account the following administrative costs of: -

- Assessing whether or not RMAT is processing the information requested;
- Locating, retrieving, and extracting the information;
- Redacting the information;
- Photocopying, printing, postage, and other costs of transferring the information to the requester;
- Equipment and supplies (e.g. discs or envelopes);
- Communicating a response to an individual, including contacting them to confirm we hold the information;
- Staff time involved in the above

84. RMAT will usually charge a fee where the response to the request is likely to take more than 18 working hours to respond to, taking into account the above. RMAT charge for staff time is £25 per hour of staff time taken. If the requester wishes RMAT to provide hard copies of documents the following charges will apply: -

Type of Charge	Charge	Basis of Charge
Disbursement Costs	Black and White Photocopying/Printing	10p per sheet
	Colour Photocopying/Printing	15p per sheet
	Other items	Actual cost
	Postage	Actual cost of Royal Mail 2nd Class postage

85. RMAT may impose a fee to comply with requests for further copies of the same information. Where RMAT requests any fee to be paid it will wherever possible suggest to the requester what information it may be able to provide without charging a fee. In the event that a large quantity of information is being processed about an individual, RMAT will ask the individual to specify the information the request is in relation to.

86. All requests will be responded to without delay and ordinarily within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

87. RMAT may still refuse to disclose information where it:

- May cause harm to the physical or mental health of another student or individual.
- Would reveal that a child is at risk of abuse, or the disclosure of such information would not be in the child's best interests.
- Is contained in Court records or a Court Order which RMAT has been made aware of or the information has been given in court proceedings concerning a child
- If RMAT refuses an SAR on any of the above grounds, the individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

Parental requests to see Educational records

88. Those with Parental Responsibility have a legal right to access to their student's educational record within 15 school days of receipt of a request.

89. Where parents fall out with each other, RMAT will follow Department for Education Guidance on understanding and dealing with issues relating to Parental Responsibility when one parent makes requests to access the record.

90. Any requests received by staff should be referred to the DPO before any information is provided.

Requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

91. Freedom of Information requests should be made to the DPO in accordance with RMATs Freedom of Information Policy.

92. We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability. We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied. Any charges will be formulated taking into account the limits set by the legislation.

Statutory Requests for Information

93. A statutory request for information is a request for information about a member of staff, student, or group of students from a statutory body.

94. Before information is shared with a statutory body, an Academy should ensure they have identified an appropriate lawful basis for processing, or an exemption, and that this is recorded.

95. Should anybody require assistance as how to action and record responses to statutory requests for information, they should contact the DPO.

Police Requests for Information

96. Where the Police or other law enforcement agencies request information from RMAT, RMAT will require the requester to provide:

- The necessary purpose for the request;
- The details of the data subject information have been requested about;
- Details of the investigation including the alleged offence;
- Details of the information requested;
- Whether informing the data subject of the request would harm the investigation;
- Whether the data subject has provided consent for the request;
- Details of the Officer in the case
- Details of the Officer authorising a request who should be the rank of inspector or above, where the data subject has not consented to the request.

Providing information over the telephone

97. RMAT staff dealing with telephone enquiries should take specific precautions to prevent the unlawful disclosure of personal data. In particular, they should:

- Verify the caller's identity to ensure information is only given to those legally entitled;

- ensure that any request that falls within the definition of a Subject Access Request is followed by the correct procedure; and

- refer to the DPO or the Academy Senior Leadership Team for assistance in difficult situations - no-one should be bullied into disclosing personal information.

Security

98. RMAT will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

99. RMAT and its Academies will have in place appropriate procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

100. Third parties with whom we contract, who will be able to access data as part of that contract, will have to undergo a due diligence check as part of our procurement process. Third parties who do not meet acceptable standards of data security will not be contracted with. If RMAT becomes aware of any data security concerns regarding a third party with whom we contract, we will reserve the right to terminate the contract.

101. Third parties are only able to access RMATs ICT systems if they have accepted that they will comply with our ICT security policies and procedures.

102. Maintaining data security means guaranteeing the confidentiality, integrity, and availability of the personal data, defined as follows:

- confidentiality - only people who are authorised to use the data can access it;
- integrity - personal data should be accurate and suitable for the purpose for which it is processed; and
- availability - authorised users should be able to access the data if they need it for authorised purposes.

103. Security procedures include the following:

- **Entry controls** Any strangers within entry-controlled areas should be reported to a senior member of staff
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Confidential paper records will not be left unattended or in clear view anywhere with general access;
- **Equipment** Data users should ensure their PC monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended;
- Electronic personal data must be coded, encrypted or password-protected;
- Personal data must be stored on the Trust network and not individual PCs or other devices;

- Where data is required to be saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use;

- **Memory sticks** should not be used. If they are needed, specific permission should be obtained from the ICT and Data Director, and they must be password- protected and fully encrypted;

- **Electronic devices** must be encrypted, or password protected and, where possible also enabled to allow the remote blocking or deletion to protect data in case of theft;

- All users including Members, Trustees and Local Review Board Members should not store personal data obtained in conducting their role on their personal devices;

- All users are provided with a secure login and are required to regularly update their password;

- **Emails** containing sensitive or confidential information must be password-protected if there are unsecure servers between the sender and recipient;

- Circular emails that contain non- Trust or Academy email addresses must be sent blind carbon copy (bcc) to prevent the disclosure of email addresses to other recipients;

- If sending confidential information by fax, staff must always check that the recipient is present at the receiving machine before sending;

- Where personal information that could be considered private or confidential is taken **off the premises**, either in electronic or paper format, staff must take the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the premises accepts full responsibility for the security of the data.

- **Document Printing** – Documents containing personal data must be collected immediately and not left on printers/photocopiers.

104. Before sharing data, all staff will ensure:

- They are allowed to share it;
- That adequate security is in place to protect it; and
- The person/organisation who will receive the data has been outlined in a Privacy Notice.

105. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of an Academy containing sensitive information should be supervised at all times.

106. The physical security of the Academy's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to ensure secure data storage will be put in place.

107. The Trust Director of ICT and Data is responsible for ensuring continuity and recovery measures are in place to provide for the security of protected data.

108. Academy Principals and the Trust Director of ICT and Data shall ensure that Trust ICT security policies and procedures are implemented.

109. Any member of staff found to be in breach of the above security measures may be subject to disciplinary action

Data Protection Impact Assessments (DPIAs)

110. RMAT takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

111. In certain circumstances the law requires us to conduct detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

112. RMAT will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered.

113. The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment. They may consult with the ICO about the same.

114. DPIAs allow RMAT to identify and resolve problems at an early stage. This will reduce associated costs, prevent risks to a Data Subjects rights or damage to the reputation of RMAT.

115. A DPIA will be conducted when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

116. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling;
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences; and
- The use of Closed-Circuit Television ("CCTV").

Data Processors

117. We contract with various organisations who provide services to RMAT, including but not limited to school meal providers, cleaning companies, IT applications.

118. In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

119. Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of RMAT. RMAT will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

120. Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

Images and videos

121. Parents and others attending RMAT events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. RMAT does not prohibit this as a matter of policy.

122. RMAT does not however agree to any such photographs or videos being used for any other purpose but acknowledges that such matters are outside of the ability of the Trust to prevent.

123. RMAT asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

124. As a Trust we want to celebrate the achievements of our students and therefore may want to use images and videos of our students within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of students, and their parents where appropriate, before allowing the use of images or videos of students for such purposes.

125. Whenever a student begins their attendance in RMAT they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that student. We will not use images or videos of students for any purpose where we do not have consent.

126. Photographic images and videos may be kept for archiving purposes, in the public interest and historical research. They will not be published within general marketing publications or the website for a period longer than 4 years after the photograph was taken.

CCTV

127. RMAT understands that recording images of identifiable individuals constitutes processing personal data and should be done in line with data protection principles.

128. RMAT notifies all students, staff, and visitors of the purpose for collecting CCTV images via signage. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

Biometric Recognition systems

129. RMAT operates a biometric recognition system for the purposes of payment of dinner monies.

130. Before we are able to obtain the Biometric Data of students or staff we are required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

131. For Staff, written consent will be obtained at the commencement of their position within RMAT and shall continue to be effective unless an objection in writing to the processing of your Biometric Data is received from the individual.

132. For students under the age of 18 years, the Academy will notify each parent of that student (that the Academy has the contact details for and is able to contact) prior to them commencing their education at the Academy of the use of our Biometric Recognition System. RMAT will then obtain the written consent of one of the student's parents before obtaining any Biometric Data.

133. In the event that written consent cannot be obtained from a parent, or any parent objects in writing or the student objects or refuses to participate in the processing of their Biometric Data, RMAT will not process the student's Biometric Data and will provide an alternative means of accessing the dinner money system by the use of a card.

134. If consent is withdrawn, any data captured will be deleted.

Accountability

135. RMAT will implement appropriate technical and organisational measures to demonstrate that data is processed in line with data protection law.

136. RMAT will provide comprehensive, clear, and transparent Privacy Notices.

137. RMAT will implement measures that meet the principles of data protection by design and data protection be default, such as:

- Data minimisation;
- Pseudonymisation;
- Transparency;
- Allowing individuals to monitor processing;
- Continuously creating and improving security features.

138. RMAT will maintain an Information Asset Register ("IAR"). The register will include the following information for each asset:

- Description and purpose of the asset;
- The owner of that asset;
- Format and location of the asset;
- Which members of RMAT staff have routine access to the information asset;
- Details of any third parties contracted to process the information;
- Retention period for the asset.

139. The IAR for each Academy will be reviewed annually and the Academy Principal will inform the DPO of any significant changes to their information assets as soon as possible.

140. Academy Principals will be the Information Asset Owner ("IAO") and responsible for all information assets in their Academy. The Chief Executive is IAO for all information assets held by RMAT centrally.

141. Academy Principals are also the day-to-day representative of RMAT as a Data Controller in their Academy.

142. Each IAO is taken to understand the value of the information that they own, and the potential risks associated with it. They are responsible for the security and maintenance of the Information Assets including ensuring other members of staff are using the information safely and responsibly,

determining the retention period for the asset and when it is destroyed ensuring this is done securely.

Data Breaches

143. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

144. The DPO, consulting with Academy Principals and the HR Team, will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their data protection training.

145. All data breaches must be notified immediately to the DPO. As much information as possible should be provided to the DPO including but not limited to: -

- The data that has been released.
- To whom it has been provided.
- If there has been any confirmation from the recipient that they have destroyed the data and if so when.

146. Where all information required is not yet known, this should not delay notification to the DPO. Initial notification may occur whilst further information is gathered by the Academy.

147. Further information on how staff should respond to Data Breaches can be found at Appendix 1.

148. Following receipt of the notification the DPO will complete a Breach Risk Assessment process to assist in the decision making regarding whether the matter is required to be reported to the ICO.

149. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be notified. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. All ICO notifiable breaches must, by law, be referred to ICO within 72 hours of RMAT becoming aware of the breach.

150. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, RMAT will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. In the event that a breach is sufficiently serious, RMAT will notify the public without undue delay.

151. All staff must assist in the effective and robust breach detection, investigation by notifying the DPO as soon as possible and co-operating in the investigation of any breach. The DPO will maintain a Log of all Data Protection Breaches of which he is notified regardless of whether the same is reported to the ICO as the ICO may wish to see the same if they audit the Trust.

152. Failure to report a notifiable breach to ICO without the statutory timescale may result in a fine, as well as a fine for the breach itself.

Data retention

153. Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Personal Data will be retained and destroyed in line with RMATs Records Management Policy which takes into account legal requirements including the Limitation Act 1980.

154. It should be noted that some records relating to former students of an Academy or employees of RMAT may be kept for an extended period for legal reasons, and to enable the provision of references or academic transcripts.

155. Paper and electronic documents/drive memories will be erased or securely destroyed once the data is no longer to be retained. Staff should seek advice from the IT Team or the DPO if they have any queries regarding the secure destruction of electronic media.

Disclosure and Barring Service ("DBS")

156. All DBS data will be managed in line with data protection legislation.

157. Any third parties who access DBS information will be made aware of the data protection legislation as well as their responsibilities as a data handler.

Complaints

158. Complaints in relation to Freedom of Information and Subject Access requests will be dealt with under RMATs complaints policy. Anyone who wishes to complain about the way RMAT has managed their personal data should contact the DPO.

Copyright

159. RMAT will take reasonable steps to inform enquirers if any third party may have a copyright or intellectual property interest in information provided in response to their requests. It will be the enquirers responsibility to ensure that any information provided by RMAT is not re-used in a way which infringes those interests, whether or not any such warning has been given.

Training

160. RMAT will ensure that appropriate guidance and training is given to the relevant staff, members of governance and other authorised 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.

161. The DPO will be consulted in relation to training where necessary; to ensure training resources and their implementation are effective.

Other Documents

162. This Policy should be read in conjunction with other documents and policies which are detailed in Appendix 2. Other documents which have informed this policy also appear in Appendix 2.

Monitoring

163. The DPO will monitor the implementation and effectiveness of the policy by monitoring reports made under the policy.

164. The DPO will monitor the relevant legislation, guidelines, and information forthcoming from the relevant statutory bodies for any recommendation or changes. Where a gap, potential inequality or shortfall in performance is identified within the policy, the DPO will advise the Board of Trustees of any changes that are needed, and a proposal will be submitted to the Trust Board within an appropriate timescale. There will be a full review of the policy by the DPO prior to the stated review date where recommendations will be made for consideration by the Trust Board.

Appendix 1 – Information Security Incident Reporting following a Data Breach

Notification and Containment

GDPR compels RMAT to report breaches of personal data to the ICO within 72 hours of discovery if the incident risks the rights and freedoms of data subjects.

Immediate Action required

If a member of staff, Member of the Trust, Trustee or Local Review Board member is made aware of an information security event (a "near miss") or an actual data breach **they must report it**. Staff should report it to their line manager or Academy Principal **and** the DPO. Governance members should report it to the DPO.

The line manager, DPO and member of staff will work together to attempt to retrieve the information and attempt to ensure that recipient parties do not possess a copy of the information.

The DPO will conduct an investigation into the breach and assign a severity rating according to the identified risks and mitigations

WHITE	Information security event No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future.
GREEN	Minimal Impact A data breach has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary.
AMBER	Moderate Impact Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. The actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office.
RED	Serious Impact A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required.

The DPO will in all incidents recommend immediate actions to those that have reported an incident, their line manager and the Information Asset Owner ("IAO").

The IAO and the DPO will be responsible for ensuring all remedial actions on white and green incidents are completed.

The DPO in all incidents rated Amber and above will inform the Chief Executive, the Trust Board Chair and the Director of HR of the incident and their recommended actions. A report on such incidents will also be provided to the Audit and Risk Committee and further investigation will be conducted by the DPO as necessary.

The Chief Executive will be responsible for ensuring all remedial actions on Amber and Red incidents are completed and suitable training is given to individual members of staff and refresher training to all staff.

Appendix 2 – Linked Documents to the Data Protection and Information Governance Policy

Trust Policies and Documents

Freedom of Information Policy and Publication Scheme
ICT and E-Safety Policy
Privacy Notice – Governance and Volunteers
Privacy Notice – Staff
Privacy Notice – Students and Families
Records Management Policy

Statutes and Secondary Legislation

Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit) Regulations 2020

General Data Protection Regulation as amended by the Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit) Regulations 2019 and the Electronic Communications (Amendments Etc) (EU Exit) Regulations 2020

Protection of Freedoms Act 2012

The Education (Pupil Information) (England) Regulations 2005

Government Guidance

Data Protection: A Toolkit for Schools

DfE Data protection for Education providers

Understanding and dealing with issues relating to parental responsibility