DATA PROTECTION & INFORMATION GOVERNANCE POLICY

The Rodillian Multi Academy Trust

Summary	Data Protection and Information Governance Policy	
Responsible Person/Author:	Head of Governance and Compliance	
Applies to: (please circle/delete as appropriate)	**Staff** ☒ **Student**☒ **Community** ☒	
Ratifying Committee(s) and Date of Final Approval:	Trust Board 10 May 2021	
Available On:	**Compliance Library** ☒	**Website** ☒
Effective from:	11 May 2021	
Date of Next Formal Review:	May 2023	
Review Period	2 years	
Status	Statutory	
Owner	The Rodillian Multi Academy Trust	
Version:	1	

DOCUMENT CONTROL

Date	Version	Action	Amendments
1	1	Policy created	Policy amended from previous Data Protection Policy

Contents

Introduction

1. This policy is to ensure the Rodillian Multi Academy Trust ("the Trust") 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"), associated guidance and Codes of Practice issued under the legislation. The policy is to be applied to the way the Trust collects, processes, holds and shares personal data and recognises the need to treat it in an appropriate and lawful manner.

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

2. This policy has due regard to data protection laws, which incorporates the GDPR and other legal requirements.

3. This policy sets out the Trust's requirements for data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

4. 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 the Trust.

5. 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").

6. This policy applies to all Members, Trustees, Local Review Board ("LRB") members and Trust staff. This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

7. 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.

Publication of this Policy

8. This policy will be brought to the attention of all Trustees, Local Review Boards, and the Principal of each Academy. The policy will be available on the Trust and Academy websites and be available to all parents and carers, students, members of the public and staff. It will also be available to Trustees, Local Review Boards and Staff in the compliance library. Following any further review of the policy resulting in an updated version being adopted by the Trust, staff and stakeholders will be advised by email where they may access it and advised whether they are required to provide confirmation that they have read the document.

3. Guidance on any aspect of this policy can be obtained from the DPO whose email address is amarham@rodillianacademytrust.co.uk.

Responsibility for this Policy

4. The Trust Board has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory or Trust framework. The Trust has delegated day to day responsibility for operating the policy to the DPO and the Principal at each Academy.

5. Academy Principals and the Chief Executive have a responsibility to ensure the fair application of this policy and all members of Academy and Central Trust staff have a responsibility for supporting colleagues and ensuring its success.

6. Trust staff are specifically responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing the Trust of any changes to their personal data;
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
  - If they have any concerns that the policy is not being followed.
  - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way.
  - If they need to rely on or capture consent, deal with data protection rights invoked by an individual or transfer personal data to a country that is not in the European Economic Area or Iceland, Liechtenstein or Norway.
  - If there has been a data breach.
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
  - If they need help with any contracts or sharing personal data with third parties.

Aims of this Policy

7. To ensure the Trust fulfils its statutory responsibilities.

8. To ensure effective security and protection for data that has been provided by individuals to the Trust which is required for the management and operation of the Trust and its establishments.

Data protection definitions

9. **Data** is information which is stored electronically or in paper based filing systems.

10. **Data Controller** – The Trust is registered with the Information Commissioner's Office ("ICO"). ICO Registration Number ZA153382 as the Data Controller for all of its Academies. As the Data Controller, it determines the purpose for which, and the manner in which, any personal data is processed.

11. **Data subjects** are the individuals about whom the personal data is held.

12. **Personal data** means data relating to a living individual who can be identified from that data or from that data and other information in the Trust's possession. Personal data can be factual such as a name, address, date of birth, internet protocol ("IP") address or it can be an opinion such as a performance appraisal.

13. **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to Personal data.

14. **Processing** is any activity that involves the use of Data. It includes obtaining, recording or holding the Data, or carrying out any operation or set of operations on the Data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal data to third parties.

15. **Special category data** includes information about a person's racial or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health condition; or sexual orientation and sex life. It also includes the processing of genetic and biometric data. Special category data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

Data Protection Principles

16. The Trust will comply with the requirements outlined in data protection law, by ensuring that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collated for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;
- Accurate and, where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard for the purposes for which it is processed, is erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed. Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interests, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by law to safeguard the rights and freedoms of individuals; and
- Processed in a manner than ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

17. The Trust, as the Data Controller, is responsible for, and able to demonstrate, compliance with the principles.

18. In applying data protection law, the Trust will also apply data protection exemptions that are provided within the law.

Accountability

19. The Trust and its Academies, will implement appropriate technical and organisational measures to demonstrate that data is processed in line with data protection law.

20. The Trust will provide comprehensive, clear and transparent Privacy Notices.

21. The Trust and its Academies, 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.

22. The Trust will develop and 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;
- Whether there is a privacy notice published for that asset;
- Which members of Trust staff have routine access to the information asset;
- Whether there are any data sharing agreements relating to the information and the name of that agreement;
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset.

23. 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.

24. 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 the Trust centrally.

25. Academy Principals are also the day to day representative of the Trust as a Data Controller in their Academy

26. 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.

27. Data Protection Impact Assessments ("DPIA's") are completed when considering using new technologies for the storage, accessing or processing of personal data, or if a new requirement for processing is likely to result in a high risk to the rights and freedoms of individuals.

28. The Trust Board is responsible for:

- Ensuring the DPO is involved where necessary in a properly and timely manner.
- Supporting the DPO to carry out their tasks by providing resources for DPO tasks and the maintenance of their knowledge.
- Not instructing the DPO in how to carry out their tasks.
- Not penalising or dismissing the DPO for performing his tasks
- Ensuring that the DPO can report directly to the Trust Board.
- Ensuring there is no conflict of interest in the duties and performance of the DPO.

DPO

29. The Trust DPO can be contacted at the registered office of the Trust:

Mr A Marham
Data Protection Officer
The Rodillian Multi Academy Trust
The Rodillian Academy
Longthorpe Lane
Lofthouse
Wakefield
WF3 3PS

Or by email amarham@rodillianacademy.co.uk or DPO@rodillianacademytrust.co.uk

30. The duties of the DPO include:

- Informing and advising the Trust and its Academies about their obligations to comply with data protections laws and regulations;
- Monitoring compliance with data protection laws and regulations, including managing internal data protection activities, advising on DPIA's and providing required training to staff;
- Acting as a point of contact for the ICO's office and data subjects;
- Developing the IAR's and Information Governance policies;
- Reporting and Investigating Information security breaches;
- Leading on information requests and information sharing arrangements;
- Reporting to Trustees on the above matters.
- Respond to requests made by Data subjects.

31. The DPO will operate independently in performing the above duties and will not be dismissed or penalised for performing their tasks.

32. Sufficient resources will be provided to the DPO to enable him to meet the obligations described above and within data protection law.

Lawful Processing

33. Data will only be lawfully processed by the Trust if one of the following conditions is satisfied where processing is necessary for:

- Compliance with a legal obligation;
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- For the performance of a contract with the data subject or to take steps to enter into a contract;
- Protecting the vital interests of a data subject or another person; or
- The purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (this condition is not available to processing undertaken by the school in the performance of its tasks).
- The consent of the data subject has been obtained.

34. Special category data will only be processed under the following conditions:

- Explicit consent of the data subject;
- Processing carried out by a not for profit body with a political, philosophical, religious or trade union aim, provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent;
- Processing relates to personal data manifestly made public by the data subject; **or**

- Processing is necessary for:

    - Carrying out obligations under employment, social security or social protection law, or a collective agreement;
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
    - Reasons of substantial public interest which is proportionate to the aim pursued and which contains appropriate safeguards;
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care systems and services or a contract with a health professional;
    - Reasons of public interest in the area of public health, such as protecting against serious cross border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices; or
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

Consent

35. Consent will only be sought prior to processing any data which cannot be done under any other

lawful basis, such as complying with a legal or regulatory requirement.

36. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

37. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

38. Where consent is given, a Consent Record should be kept that documents how, when and what type of consent was given.

39. Where the standard of consent cannot be met, processing will cease.

40. Consent provided under previous data protection legislation is reviewed to ensure it meets the standard of current data protection laws. Acceptable consent obtained under previous data protection legislation will not be reobtained.

41. Consent can be withdrawn by the individual at any time.

42. Where a student is under the age of 12, the consent of parents will be sought prior to the processing of their data.

43. When gaining consent of students who are 12 or over, consideration will be given to the age, maturity and mental capacity of the student in question. Consent will only be gained from students where it is deemed that a pupil has a sound understanding of what they are consenting to.

44. Consent for the processing of Biometric Data will be obtained from parents, regardless of a student's age.

45. The Consent will be valid for the duration of attendance at that Academy, unless consent is withdrawn or there is a notified change of Parental Responsibility.

46. If there is a disagreement over consent, or if there is no response to a consent request, it will be treated as if consent has not been given.

47. For any Looked after Children ("LAC") students, or students who are adopted, the Designated Safeguarding Lead will liaise with the student's social worker, carers or adoptive parents to establish where consent should be sought. Consideration will be given as to whether identification of a LAC student, or students who are adopted, would risk their security in any way.

The right to be informed

48. A Privacy Notice is supplied 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.

49. 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 possible consequences of failing to provide the personal data, will be provided. This information

will be supplied at the time the data is obtained.

50. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Trust 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.

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

The right to access

52. 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.

53. Requests should be made to the DPO.

54. 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 using the Parental Request for Information – Student Consent Form before releasing the information.

55. The Trust 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 the Trust's legal obligations. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

56. Any information supplied to the individual will be free of charge. The Trust may impose a fee to comply with requests for further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a fee may be charged. All fees will be based on the administrative cost of providing the information.

57. 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.

58. Where the request is manifestly unfounded or excessive, the Trust 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.

59. In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

60. The Trust 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 the Trust has been made aware of or the information has been given in court proceedings concerning a child

61. If the Trust 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

62. 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.

63. Where parents fall out with each other, the Trust will follow Department for Education Guidance on understanding and dealing with issues relating to Parental Responsibility when requests are made by one parent to access the record.

64. Any requests received by staff should be referred to the Academy Principal before any information is provided.

65. Should staff require any assistance in relation to these requests, they should contact the DPO.

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

66. Freedom of Information requests should be made to the Data Protection Officer in accordance with the Trust's Freedom of Information Policy

67. 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

The right to rectification

68. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws their consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;

- Where are processing of personal data is for direct marketing purposes and the individual objects to that processing;
- The personal data was unlawfully processed;
- The personal data is required to be erased in order to comply with a legal obligation; and
- The personal data is processed in relation to the offer of information society services to a child.

69. The Trust has a right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes; and
- The exercise or defence of legal claims.

70. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

71. Where personal data has been disclosed to third parties, they will be informed about the erasure of personal data, unless it is impossible or involves disproportionate effort to do so.

72. Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question, unless it is impossible or involves disproportionate effort to do so.

The right to restrict processing

73. Individuals have the right to block or suppress the Trust's processing of personal data.

74. In the event that processing is restricted, the Trust will store the personal data, but will not process it further, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

75. The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data;
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual;
- Where processing is unlawful and the individual opposes erasure and requests restriction instead; and
- Where the Trust no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

76. If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

77. The Trust will inform individuals when a restriction on processing has been lifted.

The right to data portability

78. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

79. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

80. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller; and
- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

81. Personal data will be provided in a structured, commonly used and machine-readable form.

82. The Trust will provide the information free of charge.

83. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations. In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

84. The Trust will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

85. Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the ICO and to a judicial remedy.

The right to object

86. The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the Privacy Notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

87. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest;
- direct marketing; or
- Processing for purposes of scientific or historical research and statistics.
- Where personal data is processed for the performance of a legal task or legitimate interests:

- an individual's grounds for objecting must relate to his or her particular situation; and
- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

88. Where personal data is processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

89. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

90. Where the processing activity outlined above is carried out online, the Trust will offer a method for individuals to object online.

Automated decision making

91. Individuals have the right not to be subject to a decision when:

- it is based on automated processing, e.g. profiling; and
- it produces a legal effect or a similarly significant effect on the individual.

92. The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

93. When automatically processing personal data for profiling purposes, the Trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact;

- Using appropriate mathematical or statistical procedures;

- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and

- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

94. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Trust has the explicit consent of the individual and

- The processing is necessary for reasons of substantial public interest.

Privacy by design and DPIA's

95. The Trust will adopt a privacy by design approach and implement technical and organisational measures that demonstrate how the Trust and its Academies have considered and integrated data protection into processing activities.

96. DPIA's will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy when new requirements with regards to data processing are identified. The Trust bases its DPIA's on ICO guidance which allows for the recording of all necessary information and for that information to be considered.

97. DPIAs will allow the Trust, and its establishments, 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 the Trust

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

99. A DPIA will be used for more than one project, where necessary.

100. 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").

101. All DPIA's should be referred to the DPO who may consult the ICO in order to seek its opinion as to whether the processing operation complies with data protection laws.

Data Breaches

102. 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.

103. The Trust DPO, liaising 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.

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

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

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.

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

106. 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.

107. 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 Star Academies becoming aware of the breach.

108. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, Star Academies 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, the Trust will notify the public without undue delay.

109. 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.

110. 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.

Security

111. The Trust 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. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

112. The Trust 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.

113. In line with the Trust's Privacy Notices, we will not share information with third parties without consent unless the law allows us to do so.

114. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures, in line with the data protection laws, an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

115. Personal data will only be transferred to a third-party data processor if that party agrees to comply with the Trust's policies and procedures on data transfer, including electronic data transfer.

116. 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 the Trust becomes aware of any data security concerns regarding a third party with whom we contract, we will reserve the right to terminate the contract.

117. Third parties are only able to access the Trust's ICT systems if they have accepted that they will comply with our ICT security policies and procedures.

118. 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.

119. Security procedures include the following:

- Entry controls are in place and any strangers within entry-controlled areas are reported;
- Confidential paper records are kept in locked drawers and cupboards, with restricted access (personal data is always considered confidential);
- Confidential paper records will not be left unattended or in clear view anywhere with general access;
- 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;
- The Trust and Academy network drives are regularly backed up off-site;
- 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 carrying out 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.

120. 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.

121. 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.

122. 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.

123. 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

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

Statutory Requests for Information

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

126. 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.

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

Providing information over the telephone

128. Trust 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.

Publication of Information

129. The Trust publishes its Freedom of Information publication scheme on its websites outlining classes of information that are made routinely available. This includes policies, annual reports and financial information. Classes of information specified in the publication scheme are made available upon request.

130. When uploading information to the Trust and Academy websites, staff should be considerate of any metadata or deletions which could be accessed in documents and images on the site.

Images: photography and videos

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

132. The Trust and its Academies, 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.

133. The Trust and its Academies will indicate its intentions for taking photographs and/or videos of pupils and will verify permission before publishing them.

134. Under data protection law, 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.

135. Where photographic images and/or video is sought for use in a publication not covered within an existing consent, specific consent should be obtained.

136. Images captured by individuals on our premises for recreational/personal purposes, made by parents/carers for family use, are exempt from data protection law.

Biometric Recognition systems

137. The Trust uses student biometric data as part of automated biometric recognition system such as students using finger prints to receive school meals instead of cash payment.

138. Written consent will be obtained before biometric data is processed. If a Parent or student does not wish to us a biometric recognition system an alternative means of accessing the service will be provided, this includes where consent has been given and then withdrawn.

139. Consent will have to be given by staff or other adults before they can use a biometric recognition system. If they do not wish to provide such consent, an alternative means of accessing the service will be provided. If consent is withdrawn, the staff or other adult may access the service using the alternative means.

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

Data retention

141. 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 the Trust's Records Management Policy which takes into account legal requirements including the Limitation Act 1980.

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

143. Retention periods will be recorded in the Trust Information Asset Register. 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")

144. All DBS data will be handled in line with data protection legislation.

145. 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

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

Copyright

147. The Trust 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 the Trust is not re-used in a way which infringes those interests, whether or not any such warning has been given.

Training

148. The Trust will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised school 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.

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

150. The Trust will ensure that any third party contractors have adequately trained their staff in Information Governance by carrying out the appropriate due diligence.

Other Documents

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

Monitoring

152. The Head of Governance and Compliance will monitor the implementation and effectiveness of the policy by monitoring reports made under the policy.

153. The Head of Governance and Compliance 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 Head of Governance and Compliance 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 Head of Governance and Compliance prior to the stated review date where recommendations will be made for consideration by the Trust Board.

Diversity

154. The Rodillian Multi Academy Trust is committed to a policy of celebrating diversity, promoting equality of opportunity, providing an inclusive workplace, and eliminating any unfair treatment or unlawful discrimination. This overriding objective applies to all policies and procedures relating to staff and students. The Trust will always comply with the requirements of the Equalities Act 2010 and associated guidance produced by the Department for Education.

Appendix 1 – Information Security Incident Reporting following a Data Breach

Notification and Containment

GDPR compels the Trust 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 carried out 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
ICT and E Safety Policy Addendum during Covid 19
Privacy Notice – Governance and Volunteers
Privacy Notice – Staff
Privacy Notice – Students
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

Department for Education ("DfE") Data Protection Policy Covid Testing Frequently Asked Questions

DfE Data protection for Education providers

DfE Privacy Notice for testing in Schools

Understanding and dealing with issues relating to parental responsibility

Appendix 3: Equality Impact Assessment

Equality, Diversity, Cohesion, and Integration Screening.

As a public authority, the Rodillian Multi Academy Trust needs to ensure that all our strategies, policies, service, and functions, both current and proposed have had proper consideration of equality, diversity, cohesion, and integration.

A **screening** process can help judge relevance and provides a record of both the **process** and **decision.** Screening should be a short, sharp exercise that determines relevance for all new and revised strategies, policies, services, and functions. Completed at the earliest opportunity it will help to determine:

- the relevance of proposals and decisions to equality, diversity, cohesion, and integration.
- whether or not equality, diversity, cohesion, and integration is being/has already been considered, and
- whether or not it is necessary to carry out an impact assessment.

Organisation: The Rodillian Multi- Academy Trust	**Department responsible for the Policy:** Head of Governance and Compliance
Lead Person: Adam Marham	**Contact Number:**

1. Title: Data Protection and Information Governance Policy

2. Please provide a brief description of what you are screening
The Policy

3. Relevance to equality, diversity, cohesion, and integration		
Questions	**Yes**	**No**
Is there an existing or likely differential impact for the different equality characteristics?		x
Have there been or likely to be any public concerns about the Policy or proposal?		x
Could the proposal affect how services are organised, provided, located and by whom?	x	
Could the proposal affect our workforce or employment practices?	x	
Does the proposal involve or will it have an impact on: - • Eliminating unlawful discrimination, victimisation, and harassment • Advancing equality of opportunity • Fostering good relations	 x	 X X

4. Considering the impact on equality, diversity, cohesion, and integration
• **Scope of the proposal:** Students, parents, staff, the community.

- **Who is likely to be affected?** Students, parents, staff, the community.
- **Consultation and engagement activities with those likely to be affected?** Ongoing feedback from Students, parents, staff, the community. The Policy is available through the Trust and Academies websites and a written copy can be provided on request.

- **Key findings**

We have considered the potential positive and negative impact on different equality characteristics in relation to the Policy and do not believe that any groups will be adversely affected. The Trust is vigilant in adhering to the appropriate legislation in relation to protected characteristics and to preventing discrimination. Managers are supported and trained in relation to these areas. The Policy has considered religious, racial and gender-specific clothing requirements and those of staff with disabilities in line with the Equality Act.

We have considered the perception that the proposal could benefit one group at the expense of another and we do not believe that the Policy could be perceived to be discriminatory with regards to its wording or format.

- **Actions**

The Trust will continue to promote positive impact and remove/reduce negative impact through the application of this Policy within the organisation.

5. Governance, ownership, and approval

Please state here who has approved the actions and outcomes of the screening

Name	**Job title**	**Date**
Adam Marham	Head of Governance and Compliance	08.04.2021

6. Publishing

This screening document will act as evidence that due regard to equality and diversity has been given.

Date screening completed	08.04.2021
Date agreed at Trust Board	10.05.2021