Romero Catholic Academy Trust

Data Protection Policy

Date of Board Approval	**November 2023**
Signature of Chair	
Version	**1**
Next review date	**As required by HY Education**
Responsible Officer	**Governance Professional**



INTRODUCTION

1. This is the Data Protection Policy of Romero Catholic Academy Trust ("the Trust" / "we" /"us").

2. We are committed to processing Personal Information fairly and lawfully in accordance with the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR"), the Data Protection Act 2018 ("the DPA") and other related legislation which protects Personal Information. It is necessary for the Trust to process Personal Information about its staff, pupils, parent(s) / guardian(s) and other individuals who it may come into contact with. In doing so, we recognise that the correct and lawful treatment of Personal Information is critical to maintaining the confidence of those connected with the Trust.

3. This Policy, and any other documents referred to in it, sets out our approach to ensuring that we comply with data protection laws. It takes account of the important requirements of the GDPR and DPA.

4. This Policy applies to the Trust and its schools. [It also applies to any subsidiaries forming part of the Trust]. Staff will be required to confirm that they have read and understood the Policy. All employees must comply with our policies and procedures relating to data protection. This Policy does not form part of any employee's contract of employment and may be amended at any time.

DEFINITION OF DATA PROTECTION TERMS

5. We have set out below some of the terms used in this Policy along with a brief explanation about what they mean.

5.1 **Data Subjects** means an identified or identifiable natural person. For example, we process personal information about parents, staff members and pupils each of whom is a data subject.

5.2 **Personal Information** means any information about a data subject. Examples of personal information could include information about a pupil's attendance, medical conditions, Special Educational Needs requirements or photographs.

5.3 **Privacy Notices** are documents provided to data subjects which explain, in simple language, what information we collect about them, why we collect it and why it is lawful to do so. They also provide other important information which we are required to provide under data protection laws.

5.4 **Data Controllers** determine the purpose and means of processing personal information. They are responsible for establishing practices and policies in line with the GDPR. The Trust is a Data Controller.

5.5 **Processing** means when personal information is used in a particular way. For example, we may need to collect, record, organise, structure, store, adapt or delete personal information. When we do this, we will be Processing.

5.6 **Special Category of Personal Information** means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data, data concerning a data subject's sex life or sexual orientation. These types of personal information are regarded as being more 'sensitive' and the law requires increased safeguards to be in place if we are to process this type of data.

DATA PROTECTION PRINCIPLES

6. When we Process Personal Information, we will do so in accordance with the 'Data Protection Principles'. In this regard, we will ensure that Personal Information is:-

   (a) Processed lawfully, fairly and in a transparent manner **(Lawfulness, Fairness and Transparency**).

   (b) Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).

   (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).

   (d) Accurate and where necessary kept up to date (**Accuracy**).

   (e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**).

   (f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

7. We are also responsible for, and required to demonstrate, our compliance with the GDPR (**Accountability**).

LEADERSHIP AND OVERSIGHT

8. The Trust Board has overall responsibility for data protection and information governance. Decision-makers are expected to lead by example and promote a proactive, positive data protection culture.

9. The Trust has a clear organisational structure with clear reporting lines and information flows between relevant groups which is set out in Appendix A.

10. Each Trust school and / or subsidiary will have a nominated lead at a local level to ensure that a strong data protection culture is established across the Trust.

11. The Policy will be reviewed and updated in accordance with documented review dates, though the Trust reserves the right to update this policy at any time where it is more immediately necessary to do so e.g. because of operational changes, court or regulatory decisions, or changes in regulatory guidance.

12. Any person who has questions regarding data protection or this policy, should contact the Trust Governance Professional who can be contacted on DPO@romerocat.com.

THE DATA PROTECTION OFFICER (DPO)

13. The GDPR requires certain organisations, including the Trust, to appoint a 'Data Protection Officer' ("DPO"). The DPO must have expert knowledge in data protection law and practices. Our appointed DPO who fulfils these requirements is HY Education, who can be contacted by telephone on 0161 543 8884 or email at DPO@wearehy.com

14. The DPO will carry out a number of important tasks which will include:-
    (a) monitoring compliance with data protection laws and our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, providing training materials and conducting internal audits.
    (b) advising on, and monitoring, data protection impact assessments.
    (c) cooperating and being the first point of contact with the Information Commissioner's Office, members of staff, parents and pupils.
    (d) Directly advise senior decision makers and raise concerns to the highest level.

15. The DPO is independent of the Trust to avoid any conflict of interest and will be given the authority, support and resources to undertake the role effectively and will report to the highest level of management in the Trust. The DPO will be involved in data protection matters in a timely manner and the Trust will have proper regard to all advice given.

ACCOUNTABILITY

16. As a Data Controller, we are responsible for, and must be able to demonstrate, compliance with the data protection principles. Examples of how we will demonstrate compliance include (but are not limited to):-

    (a) appointing a suitably qualified DPO.
    (b) implementing policies and procedures.
    (c) undertaking information audits and maintaining a record of our processing activities in accordance with Article 30 of the GDPR.
    (d) preparing and communicating Privacy Notices to Data Subjects.
    (e) providing appropriate training at regular intervals.

(f) implementing privacy by design when Processing Personal Information and completing data protection impact assessments where Processing presents a high risk to the rights and freedoms of Data Subjects.

OVERSIGHT GROUP

17. The Trust will have in place a Data Protection oversight group consisting of the DPO and members of the Trust who have key data protection duties. The Oversight Group will be chaired by the DPO

18. The purpose of the Oversight Group is monitor compliance with the UK GDPR. The Oversight Group will achieve this by assessing its compliance status against the ICO's Accountability Tracker. Minutes will be kept of each meeting.

POLICIES AND PROCEDURES

19. The Trust will implement a clear policy framework which provides staff with sufficient direction to understand their roles and responsibilities regarding data protection and information governance. Our policy framework will stem from strategic planning so that it supports the Trust's objective of creating a strong data protection culture. The Trust board has approved and endorsed the Policy, and the following policies and procedures:-

(a) Data Breach Procedures
(b) Access Procedures

(c) Records Management

(d) DPIA's

20. These policies and procedures will be reviewed and approved as part of the process outlined at paragraph 11.

TRAINING AND AWARENESS

21. The DPO will provide the Trust with appropriate training which will be rolled out to all staff. This will be provided through the DPO's HYin5ive data protection series which provides sector specific content. The HYin5ive series provides two levels of training:

    (a) A comprehensive level of training for all staff in key areas of data protection. All staff will be expected undertake this training.

    (b) An additional specialised level of training for staff in more specialised roles or roles which require a more advanced level of data protection knowledge and awareness.

22. The DPO will be responsible for keeping training provision under review. The Trust, in approving this policy, also approves the current training provision.

23. All staff are required to undertake training as part of the induction process within 1 month of their start date. Existing staff will be required to undertake refresher training once every two years unless directed otherwise. Records will be maintained to evidence that staff have received training in accordance with the Policy.

24. Staff are able an encourage to share any feedback or ideas which they feel enhance training provision across the Trust. The DPO can be contacted directly by email for this purpose at DPO@wearehy.com .

25. In addition to training, we will use a range of resources to raise awareness of data protection requirements.

TRANSPARENCY

26. We will provide appropriate privacy information to those who we process Personal Information about such as pupils, parents / carers and staff. We will provide this information in the form of a Privacy Notice, which will contain all of the necessary information required under data protection laws.

27. We will provide privacy information in a way which is effective. This means that we will proactively publish privacy information in a way which is free and easy to access. In this regard, privacy information will be made available both on our website and be available in hard copy on request. We will ensure that privacy information is set out in a way which is clear and in plain language so that that this can be easily understood.

28. We will provide privacy information in a timely manner, so that it is always available to those who we process Personal Information about.

RECORD OF PROCESSING ACTIVITIES (ROPA) AND LAWFUL BASIS FOR PROCESSING

29. The Trust will undertake information audits to ensure that it has an accurate understanding of data flows. This information will be recorded in the Trust's Article 30 Record of Processing Activities (ROPA) which will always be maintained in electronic format.

30. The ROPA will include, as a minimum, all relevant requirements of the GDPR and the legal basis upon which the Trust relies to process Personal Information. It will also record data processing activities carried by Data Processors.

31. The ROPA will be reviewed and updated at reasonable intervals.

CONSENT

32. Where it is necessary for us to obtain consent to process Personal Information, we will ensure that we do so in accordance with data protection laws. Generally, we will only obtain consent where there is not another lawful basis for Processing. An example of when we will obtain consent is if we want to place a photograph of a pupil in the newspaper, on social media or in other publications to celebrate their achievements.

33. We recognise that under data protection laws, there are stricter rules as to how consent is obtained. We will ensure that when we obtain consent, we will:-

    (a) take steps to ensure that we make it clear to Data Subjects what they are being asked to consent to.

(b) ensure that the Data Subject, either by a statement or positive action, gives their consent. We will never assume that consent has been given simply because a Data Subject has not responded to a request for consent.

(c) never use pre-ticked boxes as a means of obtaining consent.

(d) ensure that a Data Subject is informed that they can withdraw their consent at any time and the means of doing so.

(e) keep appropriate records evidencing the consents we hold.

DATA SECURITY

34. We will implement appropriate technical and organisational measures to guard against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

35. We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources and the level of risk identified.

CHANGES TO THIS POLICY

36. We reserve the right to change this policy at any time and notification of any changes will be communicated accordingly.