Polaris
Multi-Academy Trust

Policy:	GDPR Policy
Date implemented:	November 2021
Date of review:	September 2023
Date of next review:	September 2024
Lead professional:	CEO
Status:	Statutory

Index

1. Intent Statement

Polaris Multi-Academy Trust is required to keep and process certain information about its staff members, parents, governors and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

We are registered as a data controller with the Information Commissioners Office. Academies within the Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other academies or schools and educational bodies, and potentially children's services.

This policy applies to all personal data, regardless of whether it is in paper or electronic format. "Personal Data" means data which relates to a living individual who can be identified

(a) from the data

(b) from the data and other information, which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person, in respect of the individual.

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

2. Introduction

This policy covers personal data whoever the personal data belongs to and is applicable to all individual schools within the Trust. This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the core principles of the GDPR. Data Protection is the responsibility of all staff members within individual schools across the Trust

3. Monitoring and Evaluation

Monitoring and evaluation of this policy will be ongoing throughout the year and will be the responsibility of the Data Protection Officer in partnership with the leadership teams and school Administration and Finance Officers.

A central record of data protection activity including freedom of information requests, subject access requests and any breaches or near misses, will be kept and reported to the Trust Board. Any breaches of data protection regulations will be recorded and reported to the data protection officer in time to comply with the 72-hour reporting window.

Legal framework This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Data Protection Bill 2018
- The Freedom of Information Act 2000

- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Academy Standards and Framework Act 1998
- This policy will also have regard to the following guidance:
- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- IRMS Data Retention Guidance

This policy will be implemented in conjunction with the following other Academy policies:

- Retention Policy
- Photography and Videos
- E-security Policy
- ICT Acceptable Use Policy
- Freedom of Information Policy and Publication Scheme
- CCTV Policy
- Staff handbook guidance of individual schools within the Trust

4. Applicable Data

Personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These additionally include the processing of genetic data, biometric data and data concerning health matters.

Principles

In compliance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up-to-date – data that is found to be inaccurate for its purpose will either be rectified or deleted
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods due to statutory and contractual purposes and the Trust and its academies follows the IRMS data retention guidelines
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

- Always subject to some form of human processing

GDPR Individual Rights

This policy reflects the following individual rights:

- The right to be informed
- The right to erasure
- The right to access
- The right to rectification
- The right to data portability
- The right to restrict processing
- The right to object
- The right to not be the subject of any solely automated data processing (Full details of these can be found in Appendix 2)

5. Accountability

All staff are responsible for ensuring that they read this policy, the guidance in the Multi-Academy Trust handbook, and comply with it. Where a member of staff has particular responsibility for data compliance, they should make sure they understand their role. Staff are made aware that knowingly or recklessly disclosing personal data may be a criminal offence and that internal disciplinary procedures may be followed if a member of staff commits a data breach. Comprehensive, clear and transparent privacy notices will be provided to staff, pupils and parents reflecting data subjects' right to be informed. (Appendix 1)

Appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR will be implemented by each individual school within the Trust.

A 'data-flow' map and central records of data-processing activities will be maintained, including those relating to higher risk processing such as the processing of special categories data, safeguarding or that in relation to criminal convictions and offences.

The Trust will keep an Information Asset Register of data controlled by the Trust and its processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individual and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third parties, including documentation of the transfer mechanism safeguards in place

The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation through auditing and secure deletion of historic or unnecessary data from databases and sources such as MIS systems
- Transparency in systems, records and training

- Allowing individuals to monitor processing
- Continuously creating and improving security features such as migrating all email communications and sharing of data files through proprietary software
- Using data protection impact assessments where appropriate
- A central log of data processing activity will be kept for auditing purposes

6. Lawful Processing

Individual schools within the Trust will process personal data of staff and pupils for the following purposes:

- Administration of education and training
- Monitoring, reporting, calculation and publication of both exam results and references
- Safeguarding and pupil welfare
- The provision of education and training for the planning and control of the curricula and exams
- The commissioning validation and production of educational materials
- The preparation of DFES returns
- Recruitment, contractual obligations and performance management of employees
- Sub-contracting of third-party site services and contractors.

The legal basis for processing different categories of data will be identified and documented in the information asset register prior to data being processed and individuals will be informed of what data is held by the relevant individual schools in the Trust and for what purpose.

Personal data will mainly be processed under one of the following GDPR conditions:

- 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 Trust or individual school
- For the performance of a contract with the data subject or to take steps to enter into a contract
- The consent of the data subject or their parents has been obtained

The following additional conditions may also be applied in certain situations:

- Protecting the vital interests of a data subject or another person in an emergency
- For 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

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

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- 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

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 in an emergency situation.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Reasons of substantial public interest on the basis of Union or Member State law 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 or treatment or management of health or social care systems and services on the basis of Union or Member State law 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
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Consent The Trust ensures that consent mechanisms within its data collection processes meets the standards of the GDPR in that it is:

- A positive, opt-in indication
- Freely given, specific, informed and an unambiguous indication of the individual's wishes
- Recorded and securely kept as a back-up, documenting how and when consent was given
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR but acceptable consent obtained under the DPA will not be reobtained
- Able to be withdrawn by the individual at any time
- Obtained from the parents / guardians of pupils who are under the age of 16 prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child
- Obtained directly from pupils who are 16 years of age or older

7. Data Protection Officer (DPO)

The Data Protection Officer for the Trust is Peter Dawson. Heads of School acts in support of the Data Protection Officer on a day-to-day basis. Depending on the nature of the data, some of these duties may be delegated to relevant staff such as the Academy Administration and Finance Officer. the academy representative

A DPO has been appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws
- Monitor the Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members
- The DPO reports to the CEO and CFO
- The DPO will operate independently and will not be dismissed or penalised for performing their task.

The Polaris Multi Academy Trust Data Protection Officer is Pete Dawson

Email Address: Peter.Dawson@rastrick.polarismat.org.uk

8. Data Security

Individual schools within the Trust will ensure that:

- Confidential paper records will not be left unattended, in clear view and will be kept in a locked filing cabinet, drawer or safe, with restricted access
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up on school servers or cloud-based services off-site
- Memory sticks will not be used to hold personal information or in conjunction with any hardware owned by the Trust
- All electronic devices are password-protected to protect the information on the device
- Where possible, the Trust encrypts electronic devices to allow the remote blocking or deletion of data in case of theft
- Staff and governors will not use their own personal laptops or computers for Trust purposes during the school day or at any time on Trust premises
- All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their network password and data protection guidance
- Emails containing sensitive or confidential information are restricted in Microsoft 365
- When sending confidential information, staff will always check that the recipient is correct before sending
- Where it is necessary for personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Trust premises accepts full responsibility for the security of the data. Before sharing any personal data, all staff members will ensure
- That it is necessary to share the data
- They are allowed to share it
- That adequate security, such as email protection filter and / or a separate access password, is in place to protect it
- Who will receive the data has been outlined in a privacy notice
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the schools within the Trust containing sensitive information are supervised at all times.
- The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place

The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

Continuity and recovery measures are in place to ensure the security of protected data and will be enforced by the DPO in conjunction with the school Administration and Finance Officers**.**

9. Data Retention

- Data will not be kept for longer than is necessary and follow IRMS guidelines:

- Pupil and Staff Data: 7 years
- Financial Data: 6 years or as laid down by the Academies Financial Handbook
- SEN, Safeguarding, LAC and serious accidents or incidents: 25 years
- Unrequired data will be deleted as soon as practicable

Some educational records relating to former pupils or employees of the Academy may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped under confidential waste procedures, and electronic memories cleansed or destroyed, once the data should no longer be retained.

A record of confidential waste will be kept and managed by the School Business Managers. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing, consent has been withdrawn or there are legal implications.

10. Data Breaches

- 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.
- The Trust has ensured that all staff members have been made aware of, and understand, what constitutes a data breach as part of their induction and annual CPD training related to this policy.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be informed within 72 hours of the Trust becoming aware of it
- 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 by the DPO in consultation with the leadership team.
- In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust 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 public will be notified without undue delay
- Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects
- Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself

11. Data Protection Impact Assessments

Data protection impact assessments (DPIAs) will be used by schools within the Trust as needed to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur. DPIAs will be recorded within the Trust's central record of data processing activity and/or the information asset register.

A DPIA will be carried out by the Trust's DPO and appropriate staff when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one data processing activity or project, where necessary. High risk processing includes, but is not limited to, the following:

- Safeguarding
- 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
- The use of CCTV
- Requests for information from organisations such as the police, NHS or Social Services
- Issues pertaining to DBS.

The Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

12. Publication of information

In accordance with the Freedom of Information Act 2000, Polaris Multi-Academy Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request. Polaris Multi-Academy Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

Publication of information onto the website is controlled by the Trust Marketing and Communications Manager.

13. Disclosure of Data through Subject Access Requests or Freedom of Information

The GDPR right of access grants individuals the right to seek confirmation of and access to any data which is processed about them by Polaris Multi Academy Trust. Personal data will only be disclosed to third parties in two circumstances:

- Where the data subject has given consent (or in the case of a child without capacity under the Data Protection Act - ordinarily those under 12 years of age - their parent or guardian);
- Where the Trust is required or permitted by law to disclose it Polaris Multi Academy Trust and/or its academies will take reasonable steps to confirm the identity of a third party requesting personal data through either a Subject Access Request (SAR) or Freedom of Information (FOI) request and will provide advice and assistance as necessary to the requester

A Subject Access Request allows an individual:

- To verify that their data is being processed
- To access to their personal data and other supplementary data which corresponds to the information provided in the Trust's privacy notices

Where a person wishes to make a Subject Access Request, they must make a request in writing to the Trust's Data Protection Officer who will check the identity of the requester and respond in an appropriate and secure manner, ideally in person, within one month of receipt.

The DPO will clarify the exact nature and scope of the request if needed and work with the appropriate staff to collate the information. No charge will be made for a SAR unless it is deemed excessive, unfounded or repetitive in nature.

The request may be refused in whole or in part if the Trust or academy has legal grounds not to comply with the request in full. Where a request is turned down full reasons for the refusal will be given.

In the event of numerous or complex requests, the period of compliance will be extended by a further three months. An extension may also be necessary if a request is received during the summer holiday.

The individual requester 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.

Freedom of Information requests to the academies in the Trust will also be dealt with at academy level by the academy's Administration and Finance Officer. They will be responded to appropriately within the limit of 20 working days. No specific data will be collected in response to an FOI enquiry and the requester will be informed clearly whether or not the academy holds the requested information. All SAR and FOI requests and outcomes will be centrally logged.

14. CCTV

The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with GDPR principles.

The academies in the Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via its privacy notices and signage. Cameras are only placed where they do not intrude on anyone's privacy and are used to:

- Secure the safety of pupils and employees
- Assist in the management of the school
- Protect the school building and its assets from criminal damage
- Identify and prosecute offenders

All CCTV footage will be kept for 10 days for the purposes described above before being recorded over. The Site Manager is responsible for keeping the records secure and facilitating access in consultation with the Data Protection Officer.

15. Photography and Videos

The Trust and its academies will always indicate its intentions for taking photographs of pupils and will retrieve consent before publishing them. If the Trust wishes to use images/video footage of pupils in a publication, such as the academy / Trust website, prospectus, or recordings of academy plays / performances, written consent will be sought for the usage from the parent of the pupil if under 16 years of age or the individual pupil if 16 or older.

Precautions are taken when publishing photographs of pupils, in print, video or on the academy and/or Trust website. Images captured at academy events by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR but academies within the Trust will ask parents and family not to post such images online.

16. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated.

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

Recruitment

Polaris Multi-Academy Trust will collect information from candidates applying for a position. The application form will ask for information relevant to the position applied for and the applicant's explicit consent, both for the data revealed by them and for any request which will be submitted to a third party for personal data about the applicant.

The applicant will be informed of:

- Why the school/academy collects the information
- How long it will be kept
- The security in place to protect the information
- How the application will be processed
- How the information given will be verified
- They will also be informed of their right to access the data and correct any inaccuracies

All application information will be securely destroyed under confidential waste procedure unless it is needed. For further information please see the Candidate Privacy Notice.

17. Policy Review

This policy will be reviewed annually by the Trust Board.