




TRUST DATA PROTECTION POLICY

Document Control Table

Title	Academy Data Protection Policy
Author	Amarjit Cheema (Trust CEO)
Date Approved	15 th July 2024
Approved By Name	Andrew Brocklehurst (Chair of Trustees)
Signature of Approval	
Next Review Date	July 2025

Document History

Date	Author	Note of Revisions
13/06/22	S4S	4.7.39 Insert responsibility for staff to notify DPO of information rights requests. 7.4 Insert safeguarding purpose for CCTV use 10.1 Insert staff responsibility for recording information without delay 13.4 Insert Cyber-Security reviews and NCSC standards
30/06/23	S4S	4.1 Insert individuals who this policy also applies to (volunteers, Trustees, etc) 4.7.40 Insert staff to contact the DPO before engaging external services who need to access personal data. 7.4 Insert supporting behaviour management as a purpose for CCTV use 9.3 & 9.4 Insert staff responsibilities for maintaining accurate data 11.7.3 Insert require written clarification for verbal requests
11/06/24	S4S	13.8.10 Insert use of generative AI in education 19, 20 Insert/amend information requests and the rights of data subjects – details of how all rights are met

CONTENTS	PAGE
1 INTRODUCTION	3
2 ABOUT THIS POLICY.....	3
3 DEFINITION OF DATA PROTECTION TERMS	3
4 ROLES AND RESPONSIBILITIES.....	4
5 DATA PROTECTION PRINCIPLES	6
6 FAIR, LAWFUL AND TRANSPARENT PROCESSING.....	7
7 PROCESSING FOR SPECIFIED, LIMITED AND LEGITIMATE PURPOSES	8
8 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING	9
9 ACCURATE AND UP-TO-DATE DATA	9
10 TIMELY PROCESSING	9
11 PROCESSING SECURELY AND IN LINE WITH RIGHTS OF DATA SUBJECTS	10
12 NOTIFYING DATA SUBJECTS.....	12
13 DATA SECURITY.....	12
14 REGISTER OF PROCESSING ACTIVITIES.....	15
15 REGISTER OF BREACHES.....	15
16 DATA PROTECTION OFFICER.....	15
17 USING DATA PROCESSORS	16
18 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK	16
19 INFORMATION REQUESTS AND THE RIGHTS OF DATA SUBJECTS.....	17
20 RIGHT OF ACCESS (SUBJECT ACCESS) REQUESTS.....	18
21 HANDLING INFORMATION REQUESTS	19
22 DISCLOSURE AND SHARING OF PERSONAL INFORMATION	20
23 CHANGES TO THIS POLICY.....	20

1 INTRODUCTION

- 1.1 Perry Hall Multi-Academy Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with schools in the Trust. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory responsibilities.
- 1.2 Trust staff are obliged to comply with this Policy when processing Personal Data on our behalf. Any breach of this Policy by Trust staff may result in disciplinary or other action.

2 ABOUT THIS POLICY

- 2.1 The Trust holds Personal Data about current, past and prospective students, parents, employees and others with whom the Trust communicates. Personal data may be recorded on paper, stored electronically, visual media or other formats.
- 2.2 This Policy and other documents referred to in it set out the basis on which the Trust will process any Personal Data it collects from individuals, whether those data are provided to us by individuals or obtained from other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.
- 2.3 This Policy does not form part of any employee's contract of employment and may be amended at any time.
- 2.4 The Data Protection Officer is responsible for supporting the Trust with compliance with the Relevant Data Protection Laws and with this Policy. That post is held by Services4Schools Ltd. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer. The Data Protection Officer can be contacted at dpo@perryhallmat.co.uk

3 DEFINITION OF DATA PROTECTION TERMS

- 3.1 In this Policy, the functions of the Trust are the provision of education and any pastoral, business, administrative, community or similar activities associated with that provision. References to the Trust 'carrying out its functions' or similar are references to these activities.
- 3.2 References to 'we' are references to the Trust and its academies.
- 3.3 **Data Subjects** means identified or identifiable natural (living) persons whose Personal Data the Trust holds. These may be pupils, parents/carers, staff, governors, visitors etc. This Policy also refers to Data Subjects as 'individuals.'
- 3.4 **Data Controllers** are the people who, or organisations which, determine the purposes for which any Personal Data are processed, including the means of the processing. The Trust and its academies are the Data Controllers of all Personal Data used for carrying out its functions.

- 3.5 **Trust Staff** are, for the purposes of this Policy, those of our employees (at Trust or academy level) whose work involves processing Personal Data. Trust staff must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.
- 3.6 **Data Processors** include any person or organisation, who is not a member of Trust staff, which processes Personal Data on our behalf, including any external suppliers that handle Personal Data on the Trust's behalf.
- 3.7 **Privacy Notices** are documents explaining to Data Subjects how their data will be used by the Trust.
- 3.8 **Personal Data** means any information relating to an identified or identifiable natural (living) person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier
- or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 3.9 **Personal Data Breach** means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data the Trust is responsible for.
- 3.10 **Pseudonymisation** means the processing of Personal Data so that it can no longer be attributed to a specific person without the use of additional information. This additional information (or key) must be kept separately and is subject to measures to ensure that the identity of the data subject remains protected.
- 3.11 **Relevant Data Protection Law** means the Data Protection Act 2018, the UKGDPR (based on the General Data Protection Regulation ((EU) 2016/679)), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) and all applicable laws and regulations relating to the processing of Personal Data and privacy as amended, re-enacted, replaced or superseded from time to time and where applicable the guidance and codes of practice issued by the United Kingdom's Information Commissioner.
- 3.12 **Special Categories of Personal Data** (formerly known as 'sensitive Personal Data') include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and genetic or biological traits. Special Categories of Personal Data can only be processed under strict conditions.

4 ROLES AND RESPONSIBILITIES

- 4.1 This policy applies to all staff employed by Perry Hall MAT; volunteers, trainees (including students on placement); agency and supply staff; members of the governance tier (including Members, Trustees and local governors); and to external organisations or individuals working on our behalf. All staff must read this Policy carefully and make sure that they are familiar with it. Staff who do not comply with this policy may face disciplinary action in line with Perry Hall MAT's Disciplinary For Teachers and Non-Teaching Staff Policy. The ICO may also take

action against individuals who willingly misuse or unlawfully process personal data that they are responsible for.

- 4.2 Staff who believe that fellow colleagues are not complying with data protection laws and/or this Policy are encouraged to report this to the DPO at dpo@perryhallmat.co.uk or confidentially, via our MAT Whistleblowing Policy.

4.3 Perry Hall MAT Board of Trustees

Perry Hall MAT's Board of Trustees has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

4.5 Data Protection Officers (DPO)

Perry Hall MAT has appointed an internal DPO (Strategic Head of Finance & Business Administration) to support with immediate onsite compliance. This post is supported by an "external DPO" Services 4 Schools Ltd to provide specialist advice.

DPO's are responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

DPO's will provide a report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on data protection issues. The internal DPO is the first point of contact for individuals whose data the MAT processes, and for the ICO.

The MAT Data Protection Officers are contactable at dpo@perryhallmat.co.uk

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with Head at your relevant school in the first instance.

4.6 Executive Headteachers, Headteachers & Heads of School (Heads)

Heads act as representatives of the data controller, Perry Hall MAT, on a day-to-day basis and as a point of contact between the Data Protection Officer and all staff. They will support the communication of key messages, support with local compliance activities and must do all that they reasonably can to ensure that data is processed in accordance with the key data protection principles set out in law (see further at 5 below).

4.7 All staff

Staff are responsible for:

- 4.7.1 Collecting, storing and processing any personal data in accordance with this policy
- 4.7.2 Promptly informing their school and the MAT Central Business Team of any changes to their personal data, such as a change of address or contact number

- 4.7.3 Contacting the internal DPO and ensuring that the Head is copied into any correspondence, in the following circumstances:
 - 4.7.31 If there has been a data breach, a near miss, or an issue that could lead to a data breach in the future
 - 4.7.32 With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - 4.7.33 If they have any concerns that this policy is not being followed
 - 4.7.34 If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - 4.7.35 If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
 - 4.7.36 Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - 4.7.37 If they need help with any contracts or sharing personal data with third parties
 - 4.7.38 Intend to share pupil or staff data through online apps or resources (known as Information Society Services) for the purposes of delivery of the curriculum or communications with parents/carers, to ensure this is done in accordance with the ICO Children's Code
 - 4.7.39 If they receive and Information Rights Request, or a request to access records which contain personal data
 - 4.7.40 If they intend to use an external service provider who will access the personal data of staff, pupils, or their families, prior to any verbal disclosure, electronic transfer, or the sharing of manual records

4.8 The Information Commissioner (ICO)

The ICO is the regulator (Supervisory Authority) for data protection in the UK. It's role is to ensure organisations and individuals alike undertake their responsibilities around the management of personal data in accordance with the law.

5 DATA PROTECTION PRINCIPLES

- 5.1 Anyone processing Personal Data for or on behalf of the Trust must comply with the principles of good practice contained in Relevant Data Protection Law. These principles state that Personal Data must be:
 - 5.1.1 processed fairly, lawfully and transparently;
 - 5.1.2 processed for specified, limited and legitimate purposes and in an appropriate way;
 - 5.1.3 adequate, relevant and not excessive for the purposes for which they are processed;

- 5.1.4 accurate and, where necessary, kept up to date;
 - 5.1.5 not kept longer than necessary for the intended purpose of processing;
and
 - 5.1.6 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, using appropriate technical or organisational measures.
- 5.2 The Trust will keep a record of all data processing activities and must be able to demonstrate its compliance with these principles and with the wider requirements of Relevant Data Protection Law.

6 **FAIR, LAWFUL AND TRANSPARENT PROCESSING**

- 6.1 For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in Relevant Data Protection Law. These include, but are not limited to:
- 6.1.1 the individual's explicit consent to the processing for one or more specified purposes;
 - 6.1.2 that the processing is necessary for the performance of a contract with the individual or for the compliance with a legal obligation to which the Trust is subject;
 - 6.1.3 that the processing is in the public interest; or
 - 6.1.4 that the processing is in the legitimate interest of the Trust or relevant third parties to which the data are disclosed, so long as this is balanced with the rights and freedoms of the individual.
- 6.2 Where a change to a process, or introduction of a new process involving the use of large volumes of Data Processing, that is likely to pose a high risk to individuals' rights, the Trust will carry out an appropriate Privacy Impact Assessment.
- 6.3 *Special Categories of Personal Data*
- 6.4 When Special Categories of Personal Data are being processed, the individual's explicit consent to processing of those data must be obtained unless the processing:
- 6.4.1 is necessary for the purposes of carrying out the obligations and exercising specific rights of the Trust or of the individual in the field of employment and social security and social protection law;
 - 6.4.2 is necessary for the assessment of the working capacity of an individual where the individual is an employee or for the provision of health or social care;
 - 6.4.3 relates to Personal Data which are manifestly made public by the individual;

- 6.4.4 is necessary for reasons of substantial public interest; or
- 6.4.5 is necessary to protect the vital interests of the individual.
- 6.5 Processing of data relating to Criminal Convictions and Offences can only take place under control of an official authority, such as instructions from the police or an order of the court, or where UK law states that processing must take place.
- 6.5.1 This is undertaken as part of the pre-employment check process (DBS) for all staff employed by the Trust, or where it is necessary to perform such a check as required by safeguarding regulation
- 6.6 *Consent of adults and organisations*
- 6.7 Where an individual gives consent to Data Processing, that consent must be freely given, specific, informed and unambiguous and should be either in the form of a statement (whether or not prepared by the Trust) or a positive action demonstrating consent. Any requests that the Trust makes for consent must be in clear language.
- 6.8 An individual has the right to withdraw consent at any time and will be informed of this right and how to exercise it when the Trust requests consent.
- 6.9 *Consent of children and young people*
- 6.10 Where consent is used as the condition for processing personal data, parental consent must be obtained for pupils or other children aged 13, or younger.

7 PROCESSING FOR SPECIFIED, LIMITED AND LEGITIMATE PURPOSES

- 7.1 In the course of carrying out its functions, the Trust may collect and process the Personal Data set out in its information asset register. This may include data we receive directly from an individual (for example, by completing forms or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, parents/carers, other schools, the local authority or other public bodies, recruitment agencies or service providers, professional advisers and others).
- 7.2 The Trust will only process Personal Data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by Relevant Data Protection Law. We will explain those purposes to the Data Subject.
- 7.3 The Trust where the recording of images of identifiable individuals through the use of CCTV will comply with the data processing principles within this policy.
- 7.4 The use of CCTV is to ensure each site is secure, to assist in the performance of our safeguarding responsibilities and to enable our schools to implement their behaviour management procedures. The Trust will adhere to the ICO's code of practice for the use of CCTV. All Pupils, staff and visitors will be notified that CCTV is in operation via signage.
- 7.5 The Trust will ensure that all CCTV footage will be kept for up to 30 calendar days for security purposes before being deleted, unless subject to a criminal or internal investigation.

7.6 Any enquiries about CCTV systems across the Trust should be directed to the Trust's Facilities and Estates Manager, Perry Hall Multi Academy Trust, PO Box 7177, Greenacres Avenue, Wolverhampton, WV1 9DB

8 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

8.1 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the individual;

8.2 If a member of staff has any doubt as to whether any processing exceeds the purposes for which that data was originally collected, he or she should notify the Data Protection Officer.

9 ACCURATE AND UP-TO-DATE DATA

9.1 We will ensure that Personal Data we hold are accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9.2 It is the responsibility of staff to ensure that their own Personal Data is accurate and kept up to date. All staff must as a minimum check that any personal data that they provide to the Trust in connection with their employment is accurate and up to date. They must also inform the Trust of any changes their personal data that they have provided, e.g. change of address, either at the time of appointment or subsequently.

9.3 Where staff are made aware of changes to the personal data of pupils and their families, this must be updated without delay, in relevant school systems and records.

9.4 Staff who are responsible for maintaining pupil information in schools must undertake regular activities to ensure information held about pupils and their families is accurate and up to date. This includes performing scheduled data collection exercises and updating systems in a timely manner with information provided in response.

10 TIMELY PROCESSING

10.1 Staff should record changes to information without delay, using relevant school systems.

10.2 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which are no longer required. We will be guided by the Information Records Management Society guidance in respect of decision making concerning the retention of Personal Data (Schools Toolkit 2019 and Academies Toolkit 2019).

10.3 If a member of staff has any doubt as to whether any Personal Data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected, he or she should notify the Data Protection Officer.

11 PROCESSING SECURELY AND IN LINE WITH RIGHTS OF DATA SUBJECTS

11.1 We are committed to upholding the rights of individuals to access Personal Data the Trust holds on them.

11.2 We will process all Personal Data in line with individuals' rights, in particular their rights to:

11.2.1 be informed, in a manner which is concise, transparent, intelligible and easily accessible and written in clear and plain language, of the purpose, use, recipients and other processing issues relating to data;

11.2.2 receive confirmation as to whether your Personal Data is being processed by us;

11.2.3 access your Personal Data which we are processing only by formal written request. We may charge you for exercising this right if we are allowed to do so by Relevant Data Protection Law. Trust employees who receive a written request should forward it to their line managers and the Data Protection Officer immediately;

11.2.4 have data amended or deleted under certain circumstances where data is inaccurate or to have data completed where data is incomplete by providing a supplementary statement to the Trust (see also Paragraph 9);

11.2.5 restrict processing of data if one of the following circumstances applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

11.2.6 Where processing has been restricted, as above, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest and the data subject shall be informed.

11.2.7 where processing is restricted under one of the grounds in Paragraph 11.2.5, the data shall only be processed with the individual's consent or

in relation to the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or the United Kingdom;

- 11.2.8 an individual who has obtained restriction of processing under Paragraph 11.2.5 shall be informed by the Trust before the restriction of processing is lifted;
 - 11.2.9 receive data concerning the individual, which he or she has provided to the Trust and is processed by automated means, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance from the Trust;
 - 11.2.10 object to data processing on grounds relating to his or her particular situation unless the Trust demonstrates compelling legitimate grounds for processing which overrides the interests, rights and freedoms of the individual or for to the establishment, exercise or defence of legal claims; and
 - 11.2.11 not to be subject to a decision based solely on automated decision-making and profiling which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is based on the individual's explicit consent.
- 11.3 It is the responsibility of all staff to ensure that any request by an individual under Paragraph 11.1 is brought to the attention of the Data Protection Officer without undue delay.
 - 11.4 The Trust may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.
 - 11.5 The Trust shall provide information on action taken on a request under Paragraph 11.1 to the individual within one month of receipt of the request unless the Trust deems it necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.
 - 11.6 If a request under Paragraph 11.2 is unfounded or excessive, the Trust may charge a reasonable fee for providing the information or refuse the request.
 - 11.7 When receiving verbal requests, or telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:
 - 11.7.1 We will check the individual's identity to make sure that information is only given to a person who is entitled to it.
 - 11.7.2 We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.
 - 11.7.3 We will require individuals to clarify their request in writing where it is not clear what information has been asked for or which records a request relates to.

- 11.8 Our employees will refer a request to the Principal and the Data Protection Officer. Employees should not be bullied into disclosing personal information.

12 NOTIFYING DATA SUBJECTS

- 12.1 If we collect Personal Data directly from individuals, we will at the time of collection inform them about the processing including:

12.1.1 the identity and contact details for the Trust and its Data Protection Officer;

12.1.2 the purpose or purposes for which we intend to process those Personal Data;

12.1.3 the types of third parties, if any, with which we will share or to which we will disclose those Personal Data; and

12.1.4 the means, if any, by which individuals can limit our use and sharing of their Personal Data.

- 12.2 If we receive Personal Data from a source other than the individual we will, except in certain circumstances, provide the individual with the information in Paragraph 12.1 above at the following times:

12.2.1 within one month of receiving the Personal Data;

12.2.2 if the Personal Data are to be used for communication with the individual, at the time of the first communication to the individual;

12.2.3 if a disclosure to another recipient is envisaged by us, at the time of the disclosure to that recipient.

- 12.3 A notification in the form of a Privacy Notice will be in writing or via a link to our website, unless the individual requests an oral notification.

- 12.4 We will also inform individuals whose Personal Data we process that the Trust is the Data Controller with regard to those data and who the Data Protection Officer is.

13 DATA SECURITY

- 13.1 We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

- 13.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Data Processor if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures.

- 13.3 Trust staff will be issued with details of their obligations in relation to security of Personal Data.

- 13.4 The Trust will undertake regular reviews of its ICT security arrangements to maintain an awareness of risk from cyber-security threat. Appropriate measures will be implemented in line with National Centre for Cyber Security recommendations.
- 13.5 All Trust staff must:
- 13.5.1 assist the Trust in upholding individuals' data protection rights;
 - 13.5.2 only act in accordance with the Trust's instructions and authorisation;
 - 13.5.3 notify the Data Protection Officer immediately of any Personal Data Breaches, allegations of Personal Data Breaches or suspicions of Personal Data Breaches in accordance with Paragraph 13.5;
 - 13.5.4 comply at all times with the terms of any agreements with the Trust and with their responsibilities under Relevant Data Protection Law;
 - 13.5.5 satisfy the Trust, within a reasonable period following request, of their compliance with the provisions of Paragraph 13.4.4.
- 13.6 The Trust will notify the Information Commissioner's Office of any Personal Data Breaches without undue delay.
- 13.7 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:
- 13.7.1 **Confidentiality:** only people who are authorised to use the data can access them;
 - 13.7.2 **Integrity:** Personal Data should be accurate and suitable for the purpose for which they are processed;
 - 13.7.3 **Availability:** authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the Trust's central computer system instead of on individual computers, tablets or other media.
- 13.8 Security procedures include:
- 13.8.1 **Building Security and Entry controls:** any unauthorised person seen on Trust or academy premises should be reported.
 - 13.8.2 **IT Equipment:** Trust staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their computers, tablets or other devices when left unattended.
 - 13.8.3 **Appropriate Sharing and Verbal Disclosure:** When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. So, from time to time we may need to ask parents/carers additional questions, to which only he/she is likely to know the answers. Information will not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

- 13.8.4 **Secure lockable desks and cupboards:** desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential.)
- 13.8.5 **Methods of disposal:** paper documents should be shredded. Digital storage devices should be handed into to relevant staff at the academy to be securely destroyed by our IT provider when they are no longer required.
- 13.8.6 **Personal data on display:** All personal data displayed in Trust or academy buildings will be limited to what is necessary and pseudonymised where appropriate.
- 13.8.7 **Electronic Transport/Transfer of Personal Data:** Trust staff will use only approved methods to transport or transfer data e.g. One Drive (removable storage devices are not permitted including USB keys, hard drives, SD cards or other removable media).
- 13.8.8 **Photographs and Digital Images (including video and video conferencing technologies).** We use photographs and digital images for a variety of purposes across schools in the Trust, these include, but are not limited to:
- Capturing development and progress in learning
 - School prospectuses and other publications focussed on promoting the schools and the Trust
 - Supporting the delivery of remote teaching and learning
 - Videoconferencing of meetings and other events
 - Assemblies and celebration events
 - Sports days
 - School performances
 - Social Media
 - Trips and residential outings
 - Managing behaviour (CCTV)
 - Keeping Children safe (CCTV)
 - Keeping our sites secure (CCTV)
- 13.8.9 Where images of children or staff are used in public areas or made available online via publication on the school website. The school will always seek consent before images are published.
- 13.8.10 AI: Where schools in the Trust use Generative Artificial Intelligence we will follow the DfE guideline for using such technologies, including:
- protecting personal and special category data in accordance with data protection legislation
 - not allowing or causing intellectual property, including pupils' work, to be used to train generative AI models, without appropriate consent or exemption to copyright
 - reviewing and strengthening cyber security by referring to the cyber standards to reduce risk of attacks
 - following the guidance published in Keeping Children Safe In Education to ensure that children and young people are not

accessing or creating harmful or inappropriate content online, including through generative AI

13.9 The Trust shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement data-protection principles and to integrate the necessary safeguards into processing activities.

13.10 The Trust shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed.

14 REGISTER OF PROCESSING ACTIVITIES

14.1 The Trust must maintain an accurate and up-to-date Information Asset Register of processing activities carried out by the Trust.

14.2 The Trust must record the following information for each processing activity:

14.2.1 the contact details for the Trust and its Data Protection Officer;

14.2.2 the purpose or purposes for which the processing activity has occurred;

14.2.3 descriptions of the categories of individuals involved in the processing activity;

14.2.4 descriptions of the categories of Personal Data involved in the processing activity;

14.2.5 descriptions of the categories of recipients of the Personal Data involved in the processing activity;

14.2.6 details of any transfers to third countries, including documentation of the transfer mechanism safeguards in place;

14.2.7 retention schedules;

14.2.8 descriptions of technical and organisational security measures in place relating to the processing activity.

14.3 It is the responsibility of all staff, in particular the Data Protection Officer, to ensure that the register of processing activities is accurate and kept up to date.

15 REGISTER OF BREACHES

15.1 The Trust must maintain an accurate and up-to-date register of all Personal Data Breaches.

15.2 If anyone becomes aware of a data protection breach they must inform the Data Protection Officer immediately by emailing dpo@perryhallmat.co.uk

16 DATA PROTECTION OFFICER

16.1 The Data Protection Officer is responsible for ensuring compliance with Relevant Data Protection Law and with this Policy. The Data Protection Officer reports to

the Trust's Chief Executive Officer and Board of Trustees but fulfils their data protection functions independently.

- 16.2 The Data Protection Officer for Perry Hall MAT is provided by Services4 Schools Ltd and be contacted at dpo@perryhallmat.co.uk or by writing to Perry Hall Multi Academy Trust, PO Box 7177, Greenacres Avenue, Wolverhampton, WV1 9DB. Please address letters: **For the attention of the Data Protection Officer.**
- 16.3 Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.
- 16.4 Where a Personal Data Breach has occurred, it will be for the Data Protection Officer to decide whether, under the circumstances and in accordance with Relevant Data Protection Law, the individual concerned must be informed of the breach.

17 USING DATA PROCESSORS

- 17.1 The Trust retains the right to engage by written contract any person or organisation, who is not a member of Trust staff, to process Personal Data on our behalf.
- 17.2 Data Processors must:
 - 17.2.1 assist the Trust in upholding individuals' data protection rights;
 - 17.2.2 only act in accordance with the Trust's instructions and authorisation;
 - 17.2.3 maintain a written record of processing activities carried out on behalf of the Trust and provide this to the Trust within [a reasonable period] following request;
 - 17.2.4 notify the Trust of Personal Data Breaches without undue delay and maintain a register of breaches in accordance with Paragraph 14;
 - 17.2.5 comply at all times with the terms of any agreements with the Trust and with their responsibilities under Relevant Data Protection Law;
 - 17.2.6 satisfy the Trust, within a reasonable period following request, of their compliance with the provisions of Paragraph 13.4.4.

18 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

- 18.1 Individuals have particular rights with regard to transfers of their Personal Data outside the UK. Circumstances in which the Trust may need to transfer data outside the UK might include use of IT services and teaching resources that are hosted overseas, arrangement and administration of school trips and cultural exchange projects.
- 18.2 Subject to the requirements in Paragraph 13.1 above, Personal Data we hold may also be processed by staff operating outside the UK who work for us or for one of our suppliers. Those staff may be engaged, among other things, in the processing of payment details and the provision of support services.

18.3 We may transfer any Personal Data we hold to a country outside the UK provided that:

18.3.1 the transfer to the country or countries in question is permitted by Relevant Data Protection Law; and

18.3.2 any transfer to a country or countries outside the UK is subject the escalation procedure under Paragraph 18.4.

18.4 Before a transfer of Personal Data is made outside the UK, the following safeguards must be provided to ensure that the rights of Data Subjects and effective legal remedies for Data Subjects are available:

18.4.1 confirmation by implementing act by the European Commission of the adequacy of the level of protection afforded by the relevant third country

18.4.2 standard data protection Paragraphs adopted by the European Commission in accordance with Relevant Data Protection Law must be included in relevant documentation;

18.4.3 confirmation that the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject;

18.4.4 confirmation that the transfer is necessary for important reasons of public interest

18.4.5 the Data Protection Officer must authorise the transfer.

19 **INFORMATION REQUESTS AND THE RIGHTS OF DATA SUBJECTS**

19.1 We are committed to upholding the rights of individuals provisioned to individuals under Relevant Data Protection Legislation.

19.2 Requests for information made to schools in the Trust often take the following form:

19.2.1 Requests for education records.

19.2.2 Freedom of information requests.

19.2.3 Right of Access (Subject access) requests.

19.2.4 An order from a Court, or a Solicitor to the High Court

19.2.5 A formal request from the Police to access information necessary for the prevention, detection or investigation of a crime

19.3 Where a person with parental responsibility requests information about a child's educational records, then these should be handled by the appropriate relevant school and advice should be sought from the Data Protection Officer.

- 19.4 If a person makes a request for information under the Freedom of Information Act, then the information should usually be provided unless there are some specific concerns about disclosing the information. Common concerns in the school context may be that information relates to other people, is confidential or legally privileged. If a Freedom of Information request is made and there are any concerns about disclosing information, then the Data Protection Officer should be contacted.
- 19.5 If a person makes a subject access request, then they are requesting the personal information that the Trust has about them. There are exemptions to disclosing some information, but these are more limited as a person has a right to know what information is held on them. If a subject access request is made, then the Data Protection Officer should be contacted immediately.

20 **RIGHT OF ACCESS (SUBJECT ACCESS) REQUESTS**

- 20.1 Individuals (or an authorised official representative) have the right to request access to information that we hold about them.
- 20.2 If we do hold information about the individual who has made the request, we will:
- 20.2.1 Provide a description of it
 - 20.2.2 Explain why we are holding and using it, and how long we will keep it for
 - 20.2.3 Identify the source of the information
 - 20.2.4 Provide information about where the information has been shared
 - 20.2.5 Let you know if we are using the data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
 - 20.2.6 Disclose a copy of the information
- 20.3 **Other Information Rights:**
- 20.4 **The right to be informed** – We uphold this by publishing Privacy Notices and letting individuals know how their information will be used when we collect it.
- 20.5 **The right to rectification** - We uphold this right by asking relevant individuals to review the information we hold on record and updating information if they provide evidence to show it has changed
- 20.6 **The right to erasure** – We uphold this right by removing or deleting information that we are no longer required to keep, unless there is a lawful reason for us to retain this information
- 20.7 **The right to restrict processing** - We uphold this right by not using disputed information until we have confirmed what is accurate, unless it is necessary to do so
- 20.8 **The right to object to processing** – We uphold this by asking individuals to consent to some types of processing and explaining how they can amend or withdraw consent.

- 20.9 **The right not to be subject to automated decision making and profiling** – We uphold this right by letting you know if these systems are used and giving you a choice for these types of decisions to be reviewed. We also assess and scrutinise the implications of systems that process personal data using computer algorithms and AI.
- 20.10 We will process all Personal Data in line with individuals' rights, in particular their rights to:
- 20.11 To make a request to access your personal information, please contact our Data Protection Officer by emailing DPO@perryhallmat.co.uk or by writing to Perry Hall Multi Academy Trust, PO Box 7177, Greenacres Avenue, Wolverhampton, WV1 9DB.
- 20.12 When making a request you should confirm:
- 20.12.1 The types of records you wish to access
 - 20.12.2 any date periods these relate to
 - 20.12.3 Please address letters: For the attention of the Data Protection Officer.
 - 20.12.4 We may require you to provide proof of your identity, before we can comply with your request.

21 **HANDLING INFORMATION REQUESTS**

- 21.1 It is the responsibility of all staff to ensure that any request by an individual under Section 20 of this policy is brought to the attention of the Data Protection Officer without undue delay.
- 21.2 The Trust may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.
- 21.3 If a request under Paragraph 20.1 does not clearly describe the information the individual wished to access in a manner which prevents the request from being completed, the Data Protection Officer will write to the individual to seek further clarification. In this circumstance, the Trust will not process the request, until a suitable clarification of the request is received.
- 21.4 The Trust shall provide information in relation to a request made under paragraph 20.1 within one month of receipt of the request, unless the Trust deems it necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.
- 21.5 If a request under Paragraph 20.1 is unfounded or excessive, the Trust may charge a reasonable fee for providing the information or refuse the request.
- 21.6 When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:
- 21.7 We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

21.8 We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

22 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

22.1 We may share Personal Data we hold with staff at any academy within the Trust.

22.2 We may also disclose Personal Data we hold to third parties:

22.2.1 if we are under a duty to disclose or share an individual's Personal Data in order to comply with any legal obligation;

22.2.2 in order to enforce or apply any contract with the individual or other agreements; or

22.2.3 to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of child welfare and fraud protection.

22.3 We may also share Personal Data we hold with selected third parties for the purposes set out in our Privacy Notices.

23 CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time. This policy will be published on the Trust and academy website(s).