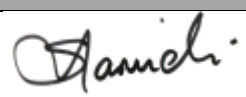
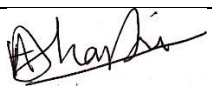
# GDPR: DATA PROTECTION POLICY

| Date this policy takes effect: | Review frequency: | Date to review: | Date to be ratified: |
|---|---|---|---|
| 19.10.2022 | Annually | Head of Estates & IT<br>Autumn 2023 | Operations Committee<br>Autumn 2023 |
| How will Trustees be assured this has been implemented? | | Through declarations of breaches, spot checks and termly reports from the DPOs of each academy | |
| Signed: |  | Sash Hamidi (EXECUTIVE HEADTEACHER) | |
| Signed: |  | Aliya Dhanji (CHAIR OF TRUSTEES) | |
| *All policies are subject to change or review in light of Government guidance or when applied.* | | | |
| *This policy works alongside the following policies:*<br>ICT & e-Safety; Business Continuity Plan; Data Retention; | | | |

**THE PEGASUS PARTNERSHIP TRUST**

*"Children First"*

## Our Vision Statement

Within The Pegasus Partnership Trust, our vision and aims of education are underpinned by the UNICEF United Nations Conventions on the Rights of the Child (UNCRC).

We believe:

- All learning should be purposeful and experiential
- In learning values and skills for whatever the future brings
- We can be world changers

**We are a PRIMARY MAT for PRIMARY SCHOOLS so every child's PRIMARY EXPERIENCE enables lifelong learning**

This means we are committed to providing an education, for all children, that should develop their personality, talents and abilities to the full (article 29). We encourage a sense of community spirit, where children pastoral care and well-being underpins academic, co-curricular and sporting excellence. We aim to achieve this through an inspiring curriculum, that is child-centred (article 3), and extends child learning beyond the constraints of the classroom. We want to instil a life-long love of learning and equip children with skills that develop their independence, critical thinking, self-awareness, resilience and self-confidence.

## Statement of intent

The Pegasus Partnership Trust aims to ensure that all personal data collected about staff, children, parents, those in governance, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. The academy may, from time to time, be required to share personal information about its staff or children with other organisations, mainly the LA, other schools and educational bodies, and potentially social services. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## Safeguarding Statement

The Pegasus Partnership Trust respects and values all children and are committed to providing a caring, friendly and safe environment for all our children so they can learn, in a relaxed and secure atmosphere (article 31). We believe every child should be able to participate in all academy activities in an enjoyable and safe environment and be protected from harm (article 19). This is the responsibility of every adult employed by, or invited to deliver services to academies within the Trust. We recognise our responsibility to safeguard all who access school and promote the welfare of all our children by protecting them from physical, sexual and emotional abuse, neglect and bullying.

## Equality Statement

At The Pegasus Partnership Trust, we ensure equality of education and opportunity for all children, staff, parents and carers receiving services from the academy, irrespective of age, race, gender (re-assignment), disability (article 23), religion and belief (article 14), sexual orientation, marital/cohabiting status or socio-economic background (article 2). We develop a culture of inclusion and diversity in which all those connected to the academy feel proud of their identity and able to participate fully in academy life.

The achievement of children is monitored by race, gender and disability and we use this data to support children, raise standards and ensure inclusive teaching. We tackle discrimination by the positive promotion of equality, challenging bullying and stereotypes and creating an environment which champions respect for all. We believe that diversity is a strength, which should be respected and celebrated by all those who learn, teach and visit here.

***This policy sets the expectation that all staff at The Pegasus Partnership Trust (the "Trust") see themselves as learners and therefore reflects their development as professionals.***

## CONTENTS

1.0 Introduction ....4
2.0 Legal Framework ....4
3.0 Applicable data ....4
4.0 Definitions ....5
5.0 Principles ....6
6.0 The Data Controller and the Designated Data Controllers ....7
7.0 Accountability ....7
8.0 Roles & Responsibilities ....8
8.1 Data Protection Officer (DPO) ....8
9.0 Lawfulness, fairness and transparency ....9
10.0 Limitation, minimisation and accuracy ....9
11.0 Consent ....10
12.0 Privacy by design and privacy impact assessments ....10
13.0 Data breaches ....11
14.0 Data security and storage of records ....12
15.0 Sharing personal data ....14
16.0 Subject access requests and other rights of individuals ....15
17.0 Children and subject access requests ....15
18.0 Responding to subject access requests ....15
19.0 Other data protection rights of the individual ....16
20.0 Parental requests to see the educational record ....17
21.0 Data checking ....17
22.0 Publication of information ....17
23.0 CCTV (Closed-Circuit Television) ....17
24.0 Photographs and videos ....18
25.0 Data retention ....18
26.0 Disclosure and Barring Scheme (DBS) data ....19
27.0 Policy review ....19
APPENDIX 1 ....20
APPENDIX 2 ....23
Appendix 1 Access to Personal Data Request
Appendix 2 Internal Data Breach Reporting Form

## 1.0 Introduction

1.1 The Pegasus Partnership Trust needs to keep certain information about its employees, children and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

1.2 To do this, The Pegasus Partnership Trust must comply with the Data Protection Principles which are set out in the General Data Protection Regulation (GDPR) 2018 (section 4.0).

1.3 The Pegasus Partnership Trust and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Trust has developed this Data Protection Policy.

## 2.0 Legal Framework

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

- The General Data Protection Regulation (GDPR)
- The Freedom of Information (FOI) 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 School Standards and Framework Act 1998

This policy meets the requirements of the GDPR and the expected provisions of the Data Protection Act (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 also reflects the ICO's code of practice for the use of surveillance cameras (see section 23.0) and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

2.1 This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Trust from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

## 3.0 Applicable data

3.1. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. 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, e.g. key-coded.

3.2. 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 specifically include the processing of genetic data, biometric data and data concerning health matters.

3.3. Processing data refers to collecting, using, disclosing, retaining or disposing of information.

## 4.0 Definitions

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |
| **Special categories of personal data** | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation |
| **Processing** | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.<br>Processing can be automated or manual. |

| | |
|---|---|
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **Data controller** | A person or organisation that determines the purposes and the means of processing of personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

## 5.0 Principles

5.1. In accordance 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; 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 purposes 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 are inaccurate, having regard to the purposes for which they are processed, are 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 personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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 GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

## 6.0 The Data Controller and the Designated Data Controllers

6.1 The Trust as a body corporate is the Data Controller, and the Trustees are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

6.2 The Trust has the following Designated Data Controllers in each Academy. They are:

- the Associate Headteacher
- the Administrators and
- the Office and Communications Manager & The Head of Estates & IT

6.3 Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be:

- The Head of Estates & IT
- Or the Associate Headteacher in the absence of the Head of Estates & IT

## 7.0 Accountability

7.1. The Pegasus Partnership Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

7.2 This policy applies to **all staff and volunteers** employed by our Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

7.3 The Board of Trustees has overall responsibility for ensuring that our academies comply with all relevant data protection obligations. They must also abide by the policy.

7.4. The Trust will provide comprehensive, clear and transparent privacy policies.

7.5. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

7.6. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures

7.7. Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

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

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

7.9. Data protection impact assessments will be used, where appropriate.

## 8.0 Roles & Responsibilities

### 8.1 Data Protection Officer (DPO)

A DPO will be 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 will report to the Executive Headteacher; within each Academy they will report to the Academy Lead
- Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

### 8.2 Academy Lead

The Associate Headteacher acts as the representative of the data controller on a day-to-day basis. They will ensure regular updates to staff using the in-academy Staff Bulletin.

### 8.3 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- 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 this 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, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- 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

## 9.0 Lawfulness, fairness and transparency

9.1. The legal basis for processing data will be identified and documented prior to data being processed. We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked an academy to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life, special education needs
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

9.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

9.3 If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

9.4 Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

## 10.0 Limitation, minimisation and accuracy

10.1. We will only collect personal data for specified, explicit and legitimate reasons.

10.2. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

10.3. Staff must only process personal data where it is necessary in order to do their jobs.

10.4. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Data Retention Policy.

## 11.0 Consent

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

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

11.3. Where consent is given, a record will be kept documenting how and when consent was given.

11.4. The Trust ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

11.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

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

11.7. The consent of parents/carers will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

## 12.0 Privacy by design and privacy impact assessments

12.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

12.2. The Trust will act in accordance with the GDPR by adopting privacy by design approach and implementing technical and organisational measures which demonstrate how each academy has considered and integrated data protection into processing activities.

12.3. Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

12.4. DPIAs will allow each academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Pegasus Partnership Trust's reputation which might otherwise occur.

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

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

12.7. 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

12.8. 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

12.9. 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.

## 13.0 Data breaches

13.1. 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.

13.2. The Associate Headteacher will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

13.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

13.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the academy becoming aware of it. Such breaches in an academy context may include, but are not limited to:

- A non-anonymised dataset being published on an academy website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of an academy laptop containing non-encrypted personal data about pupils

13.5. 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.

13.6. 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.

13.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

13.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

13.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the academy, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

13.10. 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

13.11. Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

## 14.0 Data security and storage of records

14.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Where personal information needs to be taken off site, staff must sign it in and out from the academy office
- Passwords that are at least 8 characters long containing letters and numbers are used to access academy computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Where data is 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
- Where possible, the academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff, pupils or Local Stakeholder Group Associates and/or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for academy -owned equipment (see our acceptable use agreement
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected
- Staff and Local Stakeholder Group Associates and/or Trustees will not use their personal laptops or computers for academy purposes unless using remote access however login details must not be saved on the device.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents, prospective staff etc are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- In the rare occasion of sending confidential information by fax, staff will always check that the recipient is correct before sending.
- Where 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 or on their persons for example on academy trips. The person taking the information from the academy premises accepts full responsibility for the security of the data.

14.2. Before sharing data, all staff members will ensure:

- They are allowed to share it
- That adequate security is in place to protect it
- Who will receive the data has been outlined in a privacy notice

14.3. Under no circumstances are visitors allowed access to confidential or personal information – only on a need to know basis. Visitors to areas of the academy containing sensitive information are supervised at all times.

14.4. The physical security of the academy'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.

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

## 15.0 Sharing personal data

15.1 We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/carer that puts the safety of our staff or the child or the parent at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and children – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

15.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of a potential crime and/or potential fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

15.3 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

15.4 Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## 16.0 Subject access requests and other rights of individuals

16.1. Individuals have a right to make a 'subject access request' to gain access to personal information that the academy holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

16.2. All staff, parents/carers and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form (Appendix 1) and submit it to the Data Protection Officer.

16.3 The Trust will make a charge of £25 on each occasion that access is requested, although the Trust has discretion to waive this.

16.4 The Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days. See section 16.0 for further information.

## 17.0 Children and subject access requests

17.1 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

17.2 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our academies may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

## 18.0 Responding to subject access requests

18.1. When responding to requests, we:

- May ask the individual to provide 2 forms of identification

- May contact the individual via phone to confirm the request was made and the reason why they require the information
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

18.2. We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

18.3. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

18.4. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

18.5. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

## 19.0 Other data protection rights of the individual

19.1. In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

19.2. Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## 20.0 Parental requests to see the educational record

Parents/carers, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

## 21.0 Data checking

Systems will be put in place to ensure the personal data that we hold is up to date and accurate. For example, the academy will ensure that parents are asked at least once a year to confirm their contact details. Any inaccuracies discovered or reported will be rectified as soon as possible.

## 22.0 Publication of information

22.1. The Trust publishes a publication scheme on its website & DB primary platform outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

22.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

22.3. The Pegasus Partnership Trust will not publish any personal information, such as photos and names, on its website without the permission of the affected individual.

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

## 23.0 CCTV (Closed-Circuit Television)

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

23.2. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

23.3. We use CCTV in various locations around the academy sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

23.4. All CCTV footage will be kept for a minimum length of time for security purposes.

23.5. The academies will always indicate their intentions for taking photographs of pupils and will retrieve permission before publishing them.

23.6. If an academy wishes to use images/video footage of children in a publication, such as the academy website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

23.7. Images captured by individuals for recreational/personal purposes, and videos made by parents/carers for family use, are exempt from the GDPR.

## 24.0 Photographs and videos

24.1. As part of academy activities, we may take photographs and record images of individuals within an academy.

24.2. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials when they start at the academy. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Uses may include:

- Within an academy on display boards and in academy brochures, newsletters, etc.
- Outside of an academy by external agencies such as the school photographer, newspapers, campaigns
- Online on our Trust/Academy website or social media pages

24.3. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

24.4. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. See our ICT & e-safety policy more information on our use of photographs and videos.

## 25.0 Data retention

25.1. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will destroy paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

25.2. Data will not be kept for longer than is necessary (refer to Data Retention Policy).

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

Pupil files are transferred to a child's new school once they leave the Trust. This is either hand delivered or sent recorded delivery.

25.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

## 26.0 Disclosure and Barring Scheme (DBS) data

26.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

26.2. Data provided by the DBS will never be duplicated with the exception of DBS numbers on staff and governor ID cards.

26.3. 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.

## 27.0 Policy review

27.1 The DPO is responsible for monitoring and reviewing this policy with the governing body.

27.2 This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our Trust's practice. Otherwise, or from then on, this policy will be reviewed **every year** and shared with the full governing board.

## APPENDIX 1

# ACCESS TO PERSONAL DATA REQUEST

### GENERAL DATA PROTECTION REGULATION 2018

| | |
|---|---|
| Enquirer's Surname | |
| Enquirer's Forenames | |
| Enquirer's Address | |
| Enquirer's Postcode | |
| Telephone Number | |

**Are you the person who is the subject of the records you are enquiring about?**

**YES / NO (i.e. the "Data Subject")?**

**If NO,**

**Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?**

**YES / NO**

**If YES,**

**Name and age of child or children about whose personal data records you are enquiring:**

_____

_____

**Description of Concern / Area of Concern:**

_____

_____

_____

**Description of Information or Topic(s) Requested (In your own words):**

_____

_____

_____

**Additional information including purpose for collecting this information:**

_____

_____

_____

**Please send reply to:** ***(if different from enquirer's details as stated on this form)***

Name: Mr Mark Alwyn

Address: The Pegasus Partnership Trust
c/o Priestmead Primary School
Hartford Avenue
Kenton, Harrow,
Middlesex

Postcode: HA3 8SZ

**DATA SUBJECT DECLARATION**

I request that the Academy search its records based on the information supplied above under the General Data Protection Regulation 2018 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the academy.

I agree that the reply period will commence when I have supplied sufficient information to enable the academy to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

**Signature of "Data Subject" (or Subject's Parent/Carer):** _____

**Name of "Data Subject" (or Subject's Parent/Carer) (PRINTED):** _____

**Dated:** _____

## APPENDIX 2

### DATA BREACH REPORTING FORM

| | |
|---|---|
| School/Academy | |
| Date of Breach | |
| Time of Breach | |
| Date of Breach reported to DPO | |
| Time of Breach reported to DPO | |
| Who is reporting the breach | |
| Type of Data Breach (including the categories and approximate number of individuals and records concerned) | |
| Description of the data breach | |
| Likely consequences of the data breach | |
| Description of measures to be taken to deal with breach | |
| Description of the measures taken to mitigate any possible adverse effects | |