Data Protection Policy

Contents:

1. Legal framework;
2. Applicable data;
3. Principles;
4. Accountability;
5. Data protection officer (DPO);
6. Lawful processing;
7. Consent;
8. The right to be informed;
9. The right of access;
10. The right to rectification;
11. The right to be forgotten;
12. The right to restrict processing;
13. The right to data portability;
14. The right to object;
15. Data breach/ breach management;
16. Data security;
17. Publication of information;
18. CCTV and photography;
19. Data retention;
20. DBS data;
21. Policy review.

Appendices

a. Fair processing notice;
b. Privacy notice (THNS);
c. Privacy notice (workforce);
d. HR records management protocol;
e. Retention register.

1. Legal framework

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

a) The General Data Protection Regulation (GDPR);
b) The Freedom of Information Act 2000;
c) The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016);
d) The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004;
e) The School Standards and Framework Act 1998.

1.2. This policy will also have regard to the following guidance:

a) Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
b) Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

2. Applicable data

2.1. 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.

2.2. 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. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) 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;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data held is accurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed: personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public 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;
f) 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;
g) The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. Thornton Heath Nursery School (THNS) will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

5. Data protection officer (DPO)

5.1. A DPO will be appointed in order to inform and advise THNS and its employees about their obligations to comply with the GDPR and other data protection laws.

5.2. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, data will be lawfully processed under the following conditions:

a) The consent of the data subject has been obtained;
b) THNS Fair Processing Notice (appendix A).

6.3. Sensitive data will only be processed under the following conditions:

a) Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law;
b) 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;
c) Processing relates to personal data manifestly made public by the data subject;
d) Processing is necessary for: — carrying out obligations under employment, social security or social protection law, or a collective agreement. — Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent. — The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity. — Reasons of substantial public interest 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).

7. Consent

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

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

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

8. The right to be informed

8.1. The privacy notice supplied to individuals in regard to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. THNS will verify the identity of the person making the request before any information is supplied.

9.4. A copy of the information will be supplied to the individual free of charge; however, THNS may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.7. All fees will be based on the administrative cost of providing the information.

9.8. All requests will be responded to without delay and at the latest, within one month of receipt.

9.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.10. Where a request is manifestly unfounded or excessive, THNS holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

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

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, THNS will inform them of the rectification where possible.

10.3. Where appropriate, THNS will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, THNS will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to be forgotten

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances:

a) Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
b) When the individual withdraws their consent;
c) When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
d) The personal data was unlawfully processed;
e) The personal data is required to be erased in order to comply with a legal obligation;
f) The personal data is processed in relation to the offer of information society services to a child.

11.3. THNS has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

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

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

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

11.6. Where personal data has been made public within an online environment, THNS will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress THNS's processing of personal data.

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

12.3. THNS will restrict the processing of personal data in the following circumstances:

a) Where an individual contests the accuracy of the personal data, processing will be restricted until THNS has verified the accuracy of the data;
b) Where an individual has objected to the processing and THNS is considering whether their legitimate grounds override those of the individual;

c) Where processing is unlawful and the individual opposes erasure and requests restriction instead;
d) Where THNS no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

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

13. The right to data portability

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

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

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

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

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

13.5. THNS will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. THNS is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, THNS will consider whether providing the information would prejudice the rights of any other individual.

13.9. THNS will respond to any requests for portability within 4 working weeks.

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

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

14. The right to object

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

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

a) Processing based on legitimate interests or the performance of a task in the public interest;
b) Direct marketing;
c) Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

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

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

a) THNS will stop processing personal data for direct marketing purposes as soon as an objection is received;
b) THNS cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

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

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

15. Data breaches /breach management

15.1. 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.

15.2. The DPO 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.

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

15.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of THNS becoming aware of it.

15.5. 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.

15.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

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

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

16. Data security

16.1. Confidential paper records will be kept in a locked filing cabinet or drawer with restricted access.

16.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

16.3. 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.

16.4. Data is not to be saved on removable storage or a portable device and memory sticks are not to be used.

16.5. All electronic devices are password-protected to protect the information on the device in case of theft.

16.6. Where possible, THNS enables electronic devices to allow the remote blocking or deletion of data in case of theft.

16.7. Directors, staff and Governors will use their personal laptops or computers for THNS purposes and will ensure that their devices are password protected and that information is treated the same as if they were in the office. The directors, staff and governors accept full responsibility for the security of THNS data.

16.8. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

16.9. 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. The person taking the information from the school premises accepts full responsibility for the security of the data.

16.10. Before sharing data, all staff members will ensure;

a) They are allowed to share it;
b) That adequate security is in place to protect it.

16.11. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of THNS which contain sensitive information are supervised at all times.

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

17. Publication of information

17.1. THNS publishes on its website information that will be made routinely available, including:

a) Policies and procedures;
b) Minutes of meetings;

c) Annual reports;
d) Relevant financial information.

17.2. THNS will not publish any personal information, including photos, on its website without the permission of the affected individual.

18. CCTV and photography

18.1. THNS understands that recording images of identifiable individuals counts as processing personal information and therefore this is done in line with data protection principles.

18.2. THNS notifies all pupils, staff and visitors of the purpose for collecting CCTV images via signage.

18.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

18.4 All CCTV footage will be kept for up to six months for security purposes; the DPO is responsible for keeping the records secure and allowing access.

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

19. Data retention

19.1. Data will not be kept for longer than is necessary (See Appendix C- HR Records and Management protocol and Appendix D- Retention Register)

19.2. Unrequired data will be deleted as soon as practicable.

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

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

20. DBS data

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

20.2. Data provided by the DBS will never be duplicated.

20.3 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.

Policy review

21.1 April 2018 - This policy has been reviewed and amended to comply with GDPR May 2018, adapting from the original policy produced by The Pegasus Academy Trust (PAT).

21.2. The next scheduled review date for this policy is May 2020.

Appendix A
Data Protection Act – Fair Processing Notice

1.0 Introduction

1.1 Schools, Local Authorities (LAs), the Department for Education (DfE), the government department which deals with education, the Qualifications and Curriculum Authority (QCA), Ofsted and the Learning and Skills Council (LSC) all process information on pupils in order to run the education system, and in doing so have to comply with the Data Protection Act 1998. This means, among other things, that the data held about pupils must only be used for specific purposes allowed by law. We are therefore writing to tell you about the types of data held, why that data is held, and to whom it may be passed on.

2.0 Who may hold information

2.1 Thornton Heath Nursery School (THNS) holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care and to assess how well the school as a whole is doing. This information may include contact details, correspondence concerning children, assessment results, attendance information, characteristics such as ethnicity, special educational needs/ disabilities (SEND), children who speak English as an additional language (EAL), early years pupil premium entitlement (EYPP) and any relevant medical information. From time to time schools are required to pass on some of this data to LAs, the DfE and to agencies, such as QCDA, Ofsted and EFA, which is prescribed by law. When pupils transfer to primary school or other educational establishments, information is passed to them to ensure continuity of practice. SEND information is passed directly to the Inclusion Manager or SENDCo of the new school.

2.2 The **Local Authority** (LA) uses information about pupils to carry out specific functions for which it is responsible, such as the assessment of any special educational needs the pupil may have. It also uses the information to derive statistics to inform decisions on (for example) the funding of schools, and to assess the performance of schools and set targets for them. The statistics are used in such a way that individual pupils cannot be identified from them.

2.3 **Ofsted** uses information about the progress and performance of pupils to help inspectors evaluate the work of schools, to assist schools in their self-evaluation, and as part of Ofsted's assessment of the effectiveness of education initiatives and policy. Inspection reports do not identify individual pupils.

2.4 The **Educational Funding Agency** uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of Academies. They carry out a number of compliance and assurance activities on behalf of the Secretary of State, including monitoring funding agreements and admission appeals. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion information may be shared with other Government departments or agencies strictly for statistical or research purposes only.

2.5 The **Department for Education** (DfE) uses information about pupils for research and statistical purposes, to inform, influence and improve education policy and to monitor the performance of the education service as a whole. The DfE will feed back to LAs and schools information about their pupils for a variety of purposes that will include data checking exercises, use in self-evaluation analyses and where information is missing because it was not passed on by a former school. The DfE will also provide Ofsted with pupil level data for use in school inspection. Where relevant, pupil information may also be shared with post 16 learning institutions to minimise the administrative burden on application for a course and to aid the preparation of learning plans.

2.6 Pupil information may be matched with other data sources that the Department holds in order to model and monitor pupils' educational progression; and to provide comprehensive information back to LAs and learning institutions to support their day to day business. The DfE may also use contact details from these sources to obtain samples for statistical surveys: these surveys may be carried out by research agencies working under contract to the Department and participation in such surveys is usually voluntary. The Department may also match data from these sources to data obtained from statistical surveys.

2.7 Pupil data may also be shared with other Government Departments and Agencies (including the Office for National Statistics) for statistical or research purposes only. In all these cases the matching will require that individualised data is used in the processing operation, but that data will not be processed in such a way that it supports measures or decisions relating to particular individuals or identifies individuals in any results. This data sharing will be approved and controlled by the Department's Chief Statistician.

2.8 The DfE may also disclose individual pupil information to independent researchers into the educational achievements of pupils who have a legitimate need for it for their research, but each case will be determined on its merits and subject to the approval of the Department's Chief Statistician.

3.0 Rights of access

3.1 Pupils, as data subjects, have certain rights under the Data Protection Act, including a general right of access to personal data held on them, with parents exercising this right on their behalf if they are too young to do so themselves. If you wish to access the personal data held about your child, then please contact the relevant organisation in writing:

a) your child's school at the address shown on our website – www.thns.org
b) the LA's Data Protection Officer at the Education Department, Bernard Wetherill House, 8 Mint Walk, Croydon CR0 1EA;
c) the QCDA's Data Protection Officer at ; QCDA, 53- 55 Butts Road, Earlsdon Park, Coventry CB1 3BH
d) Ofsted's Data Protection Officer at Alexandra House, 33 Kingsway, London WC2B 6SE;
e) EFA's Data Protection Officer at Sanctuary Buildings, 20 Great Smith Street, London, SW1P 3BT
f) the DfE's Data Protection Officer at DfES, Caxton House, Tothill Street, London, SW1H 9NA.

3.2 In order to fulfil their responsibilities under the Act the organisation may, before responding to this request, seek proof of the requestor's identity and any further information required to locate the information requested.

3.3 Separately from the Data Protection Act, regulations provide a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. If you wish to exercise this right you should write to the school.

4.0 Croydon Child Index

4.1 As part of the legal requirements to safeguard and promote the well – being of children, the London Borough of Croydon (Social Services and Education departments) and Croydon Primary Care NHS trust have established a Child Index. There are three main reasons why we are introducing the Child Index:

a) To help practitioners identify quickly a child with whom they have contact, and whether that child is getting the universal services (education, primary health care) to which he or she is entitled;
b) To enable earlier identification of needs and more effective action to address them by providing a means for practitioners to identify who else is involved with a child;

c) To encourage better communication and closer working between different professionals and practitioners.

4.2 The Child Index brings together basic information from Education, Social Services and the Primary Care Trust records. This will include:

a) Name;
b) Date of birth;
c) Gender;
d) Address;
e) Registered GP;
f) Health Visitor or School Nurse;
g) School attended.

4.3 The Index also holds details of previous names and addresses where appropriate. Where a child or young person is receiving additional help the Index may hold contact details for the practitioner or team involved. The Child Index will not hold any information about the child's family circumstances, individual difficulties or the reasons for any additional help.

Appendix B
Thornton Heath Nursery School Privacy Notice (THNS)

Data Protection Act 1998 and GDPR May 2018
The Pegasus Academy Trust are the Data Controller for the purposes of the Data Protection Act.

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning;
- monitor and report on their progress;
- provide appropriate pastoral care;
- claim early years funding (universal or extended hours) for your child;
- claim early years pupil premium or inclusion funding;
- Comply with the law regarding data sharing;
- Support or improve educational provision;
- Ensure no children are missing education;
- Support the primary and in year admissions process;
- Safeguard children;
- assess the quality of our services;
- Improve the education and services we provide.

This information includes contact details, assessment results, attendance information, characteristics such as ethnic group, languages spoken, special educational needs/ disabilities and any relevant medical information.

We will not give information about you to anyone outside the school without your consent unless the law and our policies permit it. We are required by law to pass some of your information to the Local Authority (LA) and the Department for Education (DFE). DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998 and GDPR 2018.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data. For more information on how this sharing process works, please visit: https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

School data is also used to support the Croydon Child Index and Children in Need Census (for further information telephone 020 8726 6000 ext 63584/61646). If you want to see a copy of the information, we hold and share about you then please contact us in writing, FAO The Data Protection Officer.

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received. If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- our local authority at https://www.croydon.gov.uk/democracy/data-protection-freedom-information/, email EducationDataQuality@croydon.gov.uk or call 02087266000 ext 64072
- the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data or call 0370 000 2288

I have read and understood the Thornton Heath Nursery School privacy notice.

_____ **Signed**

_____ **Print name**

Appendix C
Thornton Heath Nursery School Privacy Notice (workforce)

Data Protection Act 1998 and GDPR May 2018
The Pegasus Academy Trust are the Data Controller for the purposes of the Data Protection Act.

We collect and hold personal information relating to those employed to teach, or otherwise engaged to work, at our school or at the local authority. We may also receive information about workforce from their previous employers, DBS, local authority and/or the Department for Education (DfE).

The categories of school information that we process include:

- personal information (such as name, employee or teacher number, national insurance number);
- payroll information;
- relevant medical and emergency contact information;
- characteristics information (such as gender, age, ethnic group);
- contract information (such as start date, hours worked, post, roles and salary information);
- work absence information (such as number of absences and reasons);
- qualifications (and, where relevant, subjects taught).

We use workforce data to:

a) enable the development of a comprehensive picture of the workforce and how it is deployed;
b) maintain the health and safety of the workforce;
c) inform the development of recruitment and retention policies;
d) enable individuals to be paid.

Collecting workforce data

We collect personal information via staff contract forms, staff information sheets and application forms. Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. For more information please refer to our Data Protection Policy. Workforce data is stored in a locked cupboard with restricted access, or on SIMS or the school network with restricted access.

Who we share workforce information with and why

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so. We routinely share this information with:

- Local Authority – we are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- Department for Education (DfE) - The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under:
- School workforce census - We are required to share information about our school employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework. For more information, please see 'How Government uses your data' section.

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce;
- links to school funding and expenditure;
- supports 'longer term' research and monitoring of educational policy.

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis;
- producing statistics;
- providing information, advice or guidance.

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data. To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. If you want to see a copy of the information, we hold and share about you then please contact us in writing, FAO The Data Protection Officer. You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed;
- a right to seek redress, either through the ICO, or through the courts.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you want to see a copy of the information, we hold and share about you then please contact us in writing, FAO The Data Protection Officer.

I have read and understood the Thornton Heath Nursery School privacy notice (workforce).

_____ **Signed**

_____ **Print name** _____ **Date**

Appendix D
HR Records Management Protocol

1. Introduction

1.1 It is important to maintain effective systems for storing HR data, to ensure compliance with the myriad of relevant legislation and to support both sound HR administration and broader HR strategy.

1.2 Records may be hard or soft copy documents (paper files, databases, spread sheets, word processing packages, etc.) and may consist of letters, memos, emails, reports, minutes, personal records or tables of information. They may also be held in the form of tape recordings, videos, cds, microfiche or more advanced media.

1.3 The Data Protection Act 1998 applies to most HR records. The Act stipulates that data must not be kept any longer than is necessary for a particular purpose. Employees have the right to access their own records and we are obliged to ensure that data kept is accurate. Before releasing any of that data to a third party, we must seek the permission of the individual concerned.

1.4 There is a large and complex regulatory regime which impacts on the retention of records. Our protocol on each of these areas is as follows:

1.5 Table 1 – description of records

Record type	Retention Period	Reason
Recruitment: Advertisement, job description (JD), application form, references, interview notes, medical clearance, DBS record number, ID, contract, required qualifications to work, permission to work in the UK, etc. for unsuccessful candidates: for successful candidates :	 1 year after recruitment process ended Duration of employment plus 6 years	Limitation Act 1980 , for audit purposes and to allow for time limits for bringing claims
Employment: Induction checklist, offer letter, probation report, pay, enhancements, market supplements, personal info (DOB, address, etc.), internal transfers, secondments etc., OH referrals, absence, lateness, complaints , capability issues, recoverable benefits such as car loan, travel loan, relocation expenses etc., parental leave agreement, resignation letter, marital status, mortgage/accommodation references, training record, name changes, home address changes, letter to DBS reporting unsuitability to	Duration of employment plus 6 years	Limitation Act 1980. for audit purposes and to allow for time limits for bringing claims

work with children/vulnerable people, management advice, file notes, use of internet/ email acceptance, termination of employment details. requests for references and their responses, dismissal information, exit interview/ questionnaire, job description of last post held, signed code of conduct and use of email and internet policy, staff TUPE transferred, secondment agreement, appraisals, emergency contact, identification and recovery of monies owed to THNS, selection for redundancy		
Fixed term workers: Record of fixed term review meeting Outcome letters End of fixed term contract Letter making fixed term a permanent position	 1 year 1 year Termination of employment + 6 years Termination of employment + 6 years (Paper records shredded after 3 years – electronic thereafter)	Limitation Act 1980
Legal cases: ET investigations, papers and case files, compliance with statutory requests from HMRC, Benefits Agency, other authorities/agencies.	Closure of case + 6 years, regardless of outcome Paper copies always kept for full 6 years	Limitation Act 1980
Equalities Monitoring: Personal profile/ monitoring information	6 years after leaving	Equality Act 2010
Medical / Health and safety records: Accident/injury reports, RIDDOR form, risk assessments, industrial injury form, ill health retirement letter	40 years from date of last entry	COSHH, RIDDOR CAW, CLW, IRR Regs
Maternity: MATB1 form, application for maternity leave, parental leave, paternity leave, adoption leave	3 years after the end of the tax year the maternity leave ends – remove after 6 years along with rest of file Paper copies shredded after 3 years	SMP Regs
Sickness: Paid and unpaid sickness absence and pay record, doctors' certificates, self-certificates and fit notes	3 years after the end of the tax year to which sickness records relate (certificates and fit notes held by manager, not HR)	SSPay Regs
National minimum wage records: Pay history, termination pay, redundancy pay, notice pay, outstanding holiday pay	3 years after the end of the period the records cover	NMWA 1998
Working time records: Opt out agreement, flexible working arrangement, hours worked	2 years from date they were made	WT Regs

Pay: Inc.	Termination + 6 years Paper copies shredded after 3 years	Taxes Management Act 1970
Disciplinary documentation: a) Investigation and hearing records related to protection of children and vulnerable people b) Investigation records relating to bullying and Harassment c) Records where investigation concludes no further action necessary d) Record where charges are dismissed at the hearing stage e) Records where matter reaches the hearing stage and at least one allegation is upheld f) Warning and /or dismissal letters relating to protection of children and vulnerable people g) Other warning or dismissal letters	Paper original copies are always kept 15 years after case closed 6 years after case closed 6 months after case closed 6 months after case closed 2 years after case closed 15 years after end of employment 6 years after warning expires unless concern continues , in which case until case is closed	Limitation Act 1980

2. Access, Storage, Format and Destruction Methods

2.1 Subject to certain exceptions, employees have the right to access their records and we are obliged to ensure that data is accurate. Before releasing such data to a third party, we must seek permission from the individual concerned.

2.2 If employment contracts, accident records or other HR records are needed for the purposes of legal action, copies of original documents must be made available if possible (in accordance with Table 1 above) , or we have to be able to explain what happened to them, backed up by a 'statement of truth'.

2.3 When we no longer need to keep certain data, its destruction must take place securely (shredding, for example).

2.4 Further special provisions may arise which affect the retention of or access to data, e.g:

a) In the context of criminal law, the Anti-Terrorism, Crime and Security Act 2001 provides a lengthy code of practice for voluntary retention of communications data;

b) To provide security services with a reliable log of phone calls, telecoms companies must keep telephone call logs for a year. Internet service providers must retain comms data for a year;

c) In the field of immigration, the UK Borders Act 2007 and the Immigration, Asylum and Nationality Act 2006 may enable access to HR records in certain circumstances.

Appendix E
Retention Register

Thornton Heath Nursery School follows retention advice from the 'Information Management Toolkit for Schools'. This has been created to assist schools to manage their information in line with the current legislative frameworks.

Module 1 consists of the base toolkit designed to assist schools under local authority control in their compliance with data protection, freedom of information and other related legislation.

Module 2 consists of additional information which is designed to assist Academies in their compliance with data protection and freedom of information legislation as well as business requirements. (In development)

Module 3 consists of additional information which is designed to assist independent schools to manage their records in line with legislative requirements. (In development)

The Information Management Toolkit for Schools is available to schools free of charge in PDF format via this weblink - http://irms.org.uk/page/SchoolsToolkit