Wembley Multi-Academy Trust

ACHIEVEMENT FOR ALL

DATA PROTECTION POLICY

Date reviewed: September 2024

Date of next review: September 2025

This policy has been drafted in accordance with the requirements of the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 and shall come into effect from 25th May 2018.

Contents

1. POLICY STATEMENT

1.1 Wembley Multi-Academy Trust (the "Trust") collects, stores, processes and retains data relating to many educational functions. Some of this data is **personal data**, and this policy sets out the principles by which we will process your data.

1.2 This policy applies to all schools within the Wembley Multi-Academy Trust.

1.3 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a Trust we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

1.4 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.5 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.6 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf.

1.7 Any breach of this policy may result in disciplinary or other action.

2. ABOUT THIS POLICY

2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the Data Protection Act 2018, and other regulations (together '**Data Protection Legislation**').

2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the *Appendix 1* to this policy.

4. DATA PROTECTION OFFICER

4.1 As a Trust, we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Matthew Lantos, and they can be contacted at dpo.lantos@bsp.london

4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy.

4.3 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.4 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

5. DATA PROTECTION PRINCIPLES

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

- **processed** fairly and lawfully and transparently in relation to the **data subject**;
- **processed** for specified, lawful purposes and in a way, which is not incompatible with those purposes;
- adequate, relevant and not excessive for the purpose;
- accurate and up to date;
- not kept for any longer than is necessary for the purpose; and
- **processed** securely using appropriate technical and organisational measures.

5.2 **Personal Data** must also:

- be **processed** in line with **data subjects'** rights;
- not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing** of **personal data** by the Trust.

6. FAIR AND LAWFUL PROCESSING

6.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

- that the **personal data** is being **processed**;
- why the **personal data** is being **processed**;
- what the lawful basis is for that **processing** (see below);
- whether the **personal data** will be shared, and if so with whom;
- the period for which the **personal data** will be held;
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

6.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

- where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
- where the **processing** is necessary to comply with a legal obligation or legitimate business interest that we are subject to, (e.g. the Education Act 2011);
- where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and
- where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**

6.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

- where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
- where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
- where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

6.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

6.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose, then they must contact the DPO before doing so.

Vital Interests

6.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.9 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

6.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

6.11 When pupils and or our **workforce** join the Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

6.12 In relation to all pupils under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.

6.13 We will generally seek consent directly from a pupil who has reached the age of 13, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

6.14 If consent is required for any other **processing** of **personal data** of any **data subject,** then the form of this consent must:

- inform the **data subject** of exactly what we intend to do with their **personal data**;
- require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- inform the **data subject** of how they can withdraw their consent.

6.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

6.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

6.17 A record must always be kept of any consent, including how it was obtained and when.

7. PROCESSING FOR LIMITED PURPOSES

7.1 In the course of our activities as a Trust, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

8. NOTIFYING DATA SUBJECTS

8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

- our identity and contact details as **Data Controller** and those of the DPO;
- the purpose or purposes and legal basis for which we intend to **process** that **personal data**;
- the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;
- whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;
- the period for which their **personal data** will be stored, by reference to our Retention and Destruction Procedure in *Appendix 2*;
- the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and
- the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter (if this is reasonable to do so), informing them of where the **personal data** was obtained from. Where possible, we will inform those providing us with **personal data** that they should notify the **data subject** before passing on **personal data** to the Trust (e.g. emergency contact details).

9. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

9.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

10. ACCURATE DATA

10.1 We will ensure that **personal data** we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11. TIMELY PROCESSING

11.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

12. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

12.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

- request access to any **personal data** we hold about them;
- object to the **processing** of their **personal data**, including the right to object to direct marketing;
- have inaccurate or incomplete **personal data** about them rectified;
- restrict **processing** of their **personal data**;
- have **personal data** we hold about them erased
- have their **personal data** transferred; and
- object to the making of decisions about them by automated means.

The Right of Access to Personal Data

12.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure, which can be found in *Appendix 3*.

The Right to Object

12.3 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

12.4 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

12.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

12.6 In respect of direct marketing any objection to **processing** must be complied with.

12.7 The Trust is not, however, obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

12.8 If a **data subject** informs the Trust that **personal data** held about them by the Trust is inaccurate or incomplete, then we will consider that request and provide a response within one month.

12.9 If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.

12.10 We may determine that any changes proposed by the **data subject** should not be made. If this is the case, then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

12.11 **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the Trust can continue to hold the **personal data** but not do anything else with it.

12.12 The Trust must restrict the **processing** of **personal data**:

- where it is in the process of considering a request for **personal data** to be rectified (see above);
- where the Trust is in the process of considering an objection to processing by a **data subject**;
- where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and
- where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust.

12.13 If the Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

12.14 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

12.15 **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances:

- where the **personal data** is no longer necessary for the purpose for which it was originally collected;
- when a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place;
- when a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;
- where the **processing** of the **personal data** is otherwise unlawful;
- when it is necessary to erase the **personal data** to comply with a legal obligation.

12.16 The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

- to exercise the right of freedom of expression or information;
- to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
- for public health purposes in the public interest;
- for archiving purposes in the public interest, research or statistical purposes; or
- in relation to a legal claim.

12.17 If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

12.18 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

12.19 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine-readable format, and to have this transferred to another organisation.

12.20 If such a request is made, then the DPO must be consulted.

13. DATA SECURITY

13.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**. All staff are made aware of the Acceptable Use of ICT Policy and sign to say they have read it.

13.2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

13.3 Security procedures include:

- **Entry controls.**
  a. The schools within the Trust are secure sites and all staff are vetted on entry to confirm their identity.
  b. Paper data is stored in a secure environment (locked cupboards, secure filing cabinets, etc.) and only those that should have access to the data are permitted to use them.
  c. Electronic data is stored on the schools SIMS system and access is restricted to the appropriate level. No access to the system is available outside of Trust's premises.
  d. Data held by individual departments and year groups is stored on a shared drive with access restricted to those that need it.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (**Personal data** is always considered confidential.)
- **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
- **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off / lock their PC when it is left unattended.
- **Working away from the school premises – paper documents.** The Trust recognises that staff will, from time to time, need to remove **personal data** from the Trust premises. This could, for example, be to mark work, write reports and complete assessment registers. If this is the case, the following precautions should be taken:
  a. All **personal data** shall be transported in a safe and secure manner. This means either carried in person, or locked away securely in the boot of a car while being transported.
  b. Documents should be kept in a closed folder, such as one with a zip lock, or in a closed bag. Staff should include their name and contact details in case the folder is lost.
  c. While off the Trust premises, every reasonable precaution should be taken to ensure that the documents are safe and not accessed by any unauthorised personnel. For example, they should be kept in a lockable cupboard at home, or precautions should be taken to ensure that access is not available to passers-by. They should not be left in a car overnight.
  d. If there is a breach (or a suspected breach), it should be reported to Trust's Data Protection Officer immediately.
- **Working away from the school premises – electronic working.** The Trust recognises that staff will, from time to time, need to remove **personal data** from the Trust's Premises. This is likely to involve data relating to pupils and, in some cases, staff. In order to ensure that data security is not compromised, the following procedures are in place.
  a. All **personal data** shall, at all times, remain on the Trust's computer systems. This could mean, for example, on a computer owned by the Trust, accessed on the email server from another computer, or remotely accessed using our

secure log in service provided by LGfL. It must not be stored, copied or backed up in any other platform (e.g. Dropbox, Google Drive, etc.)

b. **Personal data** should **NEVER** be emailed to personal email accounts and additional copies should never be made on any other personal devices. It is permitted to access email from personal devices providing data encryption has been enabled.

c. All reasonable precautions shall be taken to ensure that data security is not compromised with respect to **personal data**. This includes ensuring others do not have access to it by logging off / locking the computer when away from the computer, ensuring the data is not visible to passers-by, etc.

d. When using a laptop or mobile device, staff should not connect to an unsecure Wi-Fi connection, such as those often found in public places.

e. Ensure documents containing **personal data** are not sent to a public printer without you being present.

f. Do not install additional programmes or download software without the prior approval of the IT department.

g. Access, or attempt to access, websites that would otherwise be blocked when on the Trust premises.

- **Document printing.** Documents containing **personal data** should be printed on computers in offices and staff work rooms and collected immediately. No **personal data** should be printed / copied in public areas such as the staff room.
- **Emails.** The Trust's Data Protection Policy applies to all emails sent and received. You should treat emails in the same way as you would any electronic or paper records. The Data Protection Act 2018 (DPA) allows individuals to seek information about themselves including emails. Staff should therefore be able to find the information easily. The DPA also requires that personal data is kept for no longer than is necessary, and is accurate and up to date. You should deal with email records as you would with any electronic or paper record. Emails should be regularly deleted if they are not retained for a specific purpose. Where an email message has an attachment, a decision needs to be made as to whether the email message, the attachment or both, should be retained. It is most likely that the attachment will be saved as a record along with the email message which provides the context for the attachment.

13.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14. DATA PROTECTION IMPACT ASSESSMENTS

14.1 The Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

14.3 The Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

14.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

15. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

15.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Education and Skills Funding Agency, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

15.2 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

15.3 In some circumstances we will not share safeguarding information. Please refer to our Safeguarding Policy.

16. DATA PROCESSORS

16.1 We contract with various organisations who provide services to the Trust. The table below shows an example of the main services that we are currently contracting to third parties. It is not meant to act as an exhaustive list but rather as a sample of the data.

Business Function	Purpose of Processing	Data Subject
Finance	Payroll	Employees
Finance	Accounting and Finance	Employees
Finance	Data required under law to governors, ESFA, DfE, etc.	Employees
HR	References	Employees
HR	Data required under law to governors and third parties	Employees
HR	Recruitment	Employees, Potential Employees
ICT	Operational Management, Web filtering, Administration, Internet Access	Employees, Pupils, Parents
Catering	Meals and Free School Meals Provision, Payment	Employees, Pupils, Parents
Staff Wellbeing	Health Insurance and other services	Employees
Security	Safeguarding	Employees, Pupils
Communication	Effective Communication	Parents
Teaching and Learning	Online Learning	Employee, Pupils
Teaching and Learning	Extra-Curricular Activities	Pupils, Parents, Employees
Teaching and Learning	Data Management of Pupil Achievement, Attendance, Wellbeing, Behaviour, etc.	Pupils, Employees
Teaching and Learning	Quality Assurance	Pupils, Employees,
Teaching and Learning	Curriculum Management	Pupils, Employees, Parents
Teaching and Learning	Pupils Support and SEN	Pupils, Parents, Employees
Pupil Wellbeing	Safeguarding	Pupils, Employees, Parents
School Promotion	Celebrating Success, Publicity	Pupils, Employees
Governance	Reporting, Strategic Planning, Complaints, etc.	Pupils, Parents, Employees

16.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

16.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

17. IMAGES AND VIDEOS

17.1 Parents, pupils, staff, governors and visitors are not permitted to take photographs of children, unless express permission has been sought. The Trust does not agree to any such videos or images being used for any purpose by any other party, and images or videos of pupils should not be posted online or otherwise published by any third party.

17.2 As a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

17.3 Whenever a pupil begins their attendance at the Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

18. CCTV

18.1 The Trust operates a CCTV system. Please refer to the Trust CCTV Procedure. (*Appendix 4*).

19. DATA BREACH

19.1 The Trust is committed to the protection of all personal data and special category data for which we are the data control.

19.2 Any data breach (or suspected data breach) will be treated with the utmost seriousness and, if necessary, reported to the ICO.

19.3 Full details can be found in our Data Breach Notification Procedure (see *Appendix 5* for full details).

20. CHANGES TO THIS POLICY

20.1 We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

APPENDIX 1 - DEFINITIONS

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by Trust, such as staff and those who volunteer in any capacity including Governors, Trustees, Members and parent helpers.

APPENDIX 2 - RETENTION AND DESTRUCTION PROCEDURE

1. Introduction

Wembley Multi-Academy Trust (the "Trust") recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Trust and its schools. Records provide evidence for protecting the legal rights and interests of the Trust, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

2. Scope of the Policy

This policy applies to all records that are created, received or maintained by staff of the Trust in the course of carrying out its functions. It applies to all schools within the Wembley Multi-Academy Trust.
Records are defined as all those documents which facilitate the business carried out by the Trust and which are thereafter retained (for a set period if appropriate) to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically.
A small percentage of the Trust's records may be selected for permanent preservation as part of the Trust's archives and for historical research or to comply with legislation.

3. Responsibilities

The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person responsible for the record keeping and destruction within each school will be the Headteacher of the school, and for documents relating to Wembley Multi-Academy Trust, it will be the CEO.

The person responsible for records management in the school will give guidance about good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the Trust's records management guidelines.

4. Recording Systems

Information created by the Trust must be managed against the same standards regardless of the media in which it is stored.

- Maintenance of Record Keeping Systems
  It is important that filing information is properly resourced and is carried out on a regular basis. It is equally important that the files are weeded of extraneous information where appropriate on a regular basis. Removing information from a file once a Freedom of Information Request or Subject Access Request has been made is a criminal offence (unless it is part of normal processing).
    a. Applying retention periods is straightforward provided files are closed on a regular basis.
    b. Once a file has been closed, it should be moved out of the current filing system and stored either in a record room in the school or in another appropriate place until it has reached the end of the retention period.
    c. Information security is very important especially when dealing with personal information or sensitive policy information. All staff must comply with the guidelines provided in the Data Protection Policy.
    d. Information contained in email, fax should be filed into the appropriate electronic or manual filing system once it has been dealt with.

5. The Safe Disposal of Information Using the Retention Schedule

Files should be disposed of in line with the attached retention schedule (see *Appendix 6*). This is a process which should be undertaken on an annual basis at the end of the academic year.

Paper records containing personal information should be shredded using a cross-cutting shredder. Other files can be bundled up and put in a skip or disposed of to the waste paper merchant. Loose papers should not be put in skips unless the skip has a lid. CD's/DVD's should be cut into pieces. Audio/Video tapes and fax rolls should be dismantled and destroyed.

Electronic data should be archived on electronic media and 'deleted' appropriately at the end of the retention period. The Trust may choose to keep certain forms of communication, including **personal data** for a longer period if it is felt that this is in the legitimate interests of the Trust (for example, defending a potential claim in the future).

6. Monitoring and Review

The day-to-day monitoring and implementation of this policy is delegated to the Headteacher of the school and, where appropriate, the CEO of the Trust. This policy should be reviewed annually by the Board of Trustees and in conjunction with the Data Protection Policy.

APPENDIX 3 - SUBJECT ACCESS REQUESTS PROCEDURE

1. Policy Statement

All **Data Subjects** have rights of access to their **personal data**. This document sets out the procedure to be followed in relation to any requests made for the disclosure of **personal data processed** by the Trust.

2. Definition of data protection terms

All defined terms in this policy are indicated in bold text, and a list of definitions is included in *Appendix 1* to this policy.

3. Recognising a subject access request

- As Trust **processes personal data** concerning **data subjects**, those **data subjects** have the right to access that **personal data** under Data Protection law. A request to access this personal data is known as a Subject Access Request or SAR.
- A **data subject** is generally only entitled to access their own **personal data**, and not to information relating to other people.
- Any request by a **data subject** for access to their **personal data** is a SAR. This includes requests received in writing, by email, and verbally.
- If any member of our **workforce** receives a request for information they should inform their line manager and the Data Protection Officer ("DPO") as soon as possible.
- In order that the Trust is properly able to understand the nature of any SAR and to verify the identity of the requester, any requester making a request verbally should be asked to put their request in writing and direct this to the DPO.
- A SAR will be considered and responded to in accordance with the Data Protection Law.
- Any SAR must be notified to the DPO at the earliest opportunity.

4. Verifying the identity of a Requester

- The Trust is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are.
- Where the Trust has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two or more of the following:
    - Current passport
    - Current driving licence
    - Recent utility bills with current address
    - Birth/marriage certificate
    - P45/P60
    - Recent credit card or mortgage statement
- If the Trust is not satisfied as to the identity of the requester then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of **personal data** resulting to a data breach.

5. Fee for Responding to Requests

- The Trust will usually deal with a SAR free of charge.
- Where a request is considered to be manifestly unfounded or excessive a fee may be requested. Alternatively, the Trust may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable the Trust will inform the requester, why this is considered to be the case.
- A fee will also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

6. Time Period for Responding to a SAR

- The Trust has one month to respond to a SAR. This will run from the later of:
  a. the date of the request,
  b. the date when any additional identification (or other) information requested is received, or
  c. payment of any required fee.
- In circumstances where the Trust is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third-party requester the written authorisation of the **data subject** has been received (see below in relation to sharing information with third parties).
- The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.
- Where a request is considered to be sufficiently complex as to require an extension of the period for response, the Trust will notify the requester within one calendar month of receiving the request, together with reasons as to why this is considered necessary.

7. Form of Response

- A requester can request a response in a particular form. In particular, where a request is made by electronic means then, unless the requester has stated otherwise, the information should be provided in a commonly readable format.

8. Sharing Information with Third Parties

- **Data subjects** can ask that you share their **personal data** with another person such as an appointed representative (in such cases you should request written authorisation signed by the **data subject** confirming which of their **personal data** they would like you to share with the other person).
- Equally if a request is made by a person seeking the **personal data** of a **data subject**, and which purports to be made on behalf of that **data subject**, then a response must not be provided unless and until written authorisation has been provided by the **data subject**. The Trust should not approach the **data subject** directly but should inform the requester that it cannot respond without the written authorisation of the **data subject**.
- If the Trust is in any doubt or has any concerns as to providing the **personal data** of the **data subject** to the third party, then it should provide the information requested directly to the **data subject**. It is then a matter for the **data subject** to decide whether to share this information with any third party.
- **Personal data** belongs to the **data subject**, and in the case of the **personal data** of a child regardless of their age the rights in relation to that **personal data** are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the **personal data** of their child.
- However, there are circumstances where a parent can request the **personal data** of their child without requiring the consent of the child. This will depend on the maturity of the child and whether the Trust is confident that the child can understand their rights. Generally, where a child is under 13 years of age they are deemed not to be sufficiently mature as to understand their rights of access and a parent can request access to their **personal data** on their behalf.
- In relation to a child 13 years of age or older, then provided that the Trust is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the Trust will require the written authorisation of the child before responding to the requester, or provide the **personal data** directly to the child in accordance with the process above.
- In all cases the Trust should consider the particular circumstances of the case, and the above are guidelines only.

9. Withholding Information

- There are circumstances where information can be withheld pursuant to a SAR. These are specific exemptions and requests should be considered on a case by case basis.
- Where the information sought contains the **personal data** of third party **data subjects** then the Trust will:
    a. Consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information;
    b. If this is not possible, consider whether the consent of those third parties can be obtained; and
    c. If consent has been refused, or it is not considered appropriate to seek that consent, then to consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not, then the information may be withheld.
- So far as possible the Trust will inform the requester of the reasons why any information has been withheld.
- Where providing a copy of the information requested would involve disproportionate effort the Trust will inform the requester, advising whether it would be possible for them to view the documents at the Trust or seeking further detail from the requester as to what they are seeking, for example key word searches that could be conducted, to identify the information that is sought.
- In certain circumstances information can be withheld from the requester, including a **data subject**, on the basis that it would cause serious harm to the **data subject** or another individual. If there are any concerns in this regard, then the DPO should be consulted.

10. Process for dealing with a Subject Access Request

- When a subject access request is received, the Trust will:
    a. notify the DPO and relevant department heads;
    b. acknowledge receipt of the request and provide an indication of the likely timescale for a response within 5 working days;
    c. take all reasonable and proportionate steps to identify and disclose the data relating to the request;
    d. never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events – it is an offence to amend or delete data following receipt of a SAR that would not have otherwise been so amended or deleted;
    e. consider whether to seek consent from any third parties which might be identifiable from the data being disclosed;
    f. seek legal advice, where necessary, to determine whether the Trust is required to comply with the request or supply the information sought;
    g. provide a written response, including an explanation of the types of data provided and whether and as far as possible for what reasons any data has been withheld; and
    h. ensure that information disclosed is clear and technical terms are clarified and explained.

APPENDIX 4 - CCTV POLICY

1. Policy Statement

- The Trust uses Close Circuit Television ("CCTV") within the premises of the Trust. The purpose of this policy is to set out the position of the Trust as to the management, operation and use of the CCTV at the Trust.
- This policy applies to all members of our **workforce**, pupils, visitors to the Trust premises and all other persons whose images may be captured by the CCTV system.
- This policy takes account of all applicable legislation and guidance, including:
    a. General Data Protection Regulation ("GDPR");
    b. *Data Protection Act 2018* (together the Data Protection Legislation);
    c. CCTV Code of Practice produced by the Information Commissioner;
    d. Human Rights Act 1998.
- This policy sets out the position of the Trust in relation to its use of CCTV.

2. Purpose of CCTV

The Trust uses CCTV for the following purposes:

a. To provide a safe and secure environment for pupils, staff and visitors;
b. To prevent the loss of or damage to the Trust buildings and/or assets;
c. To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

3. Description of system

There are a total of 86 cameras on the premises of Wembley High Technology College and 84 on the premises of East Lane Primary School. The cameras are capable of displaying live images and also record images on to a central server.

4. Siting of Cameras

- All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.
- Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The Trust will make all reasonable efforts to ensure that areas outside of the Trust premises are not recorded.
- Notices are displayed around the site to inform pupils, employees, governors and visitors of the presence of CCTV.
- Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilet cubicles.

5. Privacy Impact Assessment

- Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the Trust to ensure that the proposed installation is compliant with legislation and ICO guidance.
- The Trust will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6. Management and Access

- The CCTV system will be managed by the ICT Manager.
- On a day to day basis the CCTV system will be operated by the ICT Manager.
- The viewing of live CCTV images will be restricted to the Leadership Team in the first instance. Images are not routinely accessed and only when there is a legitimate reason to do so (e.g. investigated a suspected crime).
- Recorded images which are stored by the CCTV system will be restricted to access by the Leadership Team.
- No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.
- The CCTV system is checked regularly by the ICT Manager to ensure that it is operating effectively.

7. Storage and Retention of Images

- Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.
- Recorded images are stored only for a period of not more than 28 days unless there is a specific purpose for which they are retained for a longer period.
- The Trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:
    a. CCTV recording systems being located in restricted access areas;
    b. The CCTV system being encrypted/password protected;
    c. Restriction of the ability to make copies to specified members of staff.
    d. A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Trust.

8. Disclosure of Images to Data Subjects

- Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.
- Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the Trust's Subject Access Request Policy.
- When such a request is made the IT Department will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.
- If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The IT Department must take appropriate measures to ensure that the footage is restricted in this way.
- If the footage contains images of other individuals, then the Trust must consider whether:
    a. The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
    b. The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
    c. If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
- A record must be kept, and held securely, of all disclosures which sets out:
    a. When the request was made;
    b. The process followed by the Leadership Team in determining whether the images contained third parties;
    c. The considerations as to whether to allow access to those images;
    d. The individuals that were permitted to view the images and when; and
    e. Whether a copy of the images was provided, and if so to whom, when and in what format.

9. Disclosure of Images to Third Parties

- The Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.
- CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
- If a request is received form a law enforcement agency for disclosure of CCTV images, then IT Department must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.
- The information above must be recorded in relation to any disclosure.
- If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10. Review of Policy and CCTV System

- This policy will be reviewed annually.
- The CCTV system and the privacy impact assessment relating to it will be reviewed annually.

11. Misuse of CCTV systems

- The misuse of CCTV system could constitute a criminal offence.
- Any member of staff who breaches this policy may be subject to disciplinary action.

12. Complaints relating to this policy

- Any complaints relating to this policy or to the CCTV system operated by the Trust should be made in accordance with the Trust Complaints Policy.

APPENDIX 5 - DATA BREACH NOTIFICATION PROCEDURE

1. Policy Statement

- Wembley Multi-Academy Trust (the "Trust") is committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.
- The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.
- All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2. About this policy

- This policy informs all of our **workforce** on dealing with a suspected or identified data security breach.
- In the event of a suspected or identified breach, Trust must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.
- Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.
- The Trust must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.
- Failing to appropriately deal with and report data breaches can have serious consequences for the Trust and for **data subjects** including:
    a. identity fraud, financial loss, distress or physical harm;
    b. reputational damage to Trust; and
    c. fines imposed by the ICO.

3. Definition of data protection terms

- All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in *Appendix 1* to this policy.

4. Identifying a Data Breach

- A data breach is a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data**.
- This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:
    a. Leaving a mobile device on a train;
    b. Theft of a bag containing paper documents;
    c. Destruction of the only copy of a document; and
    d. Sending an email or attachment to the wrong recipient;
    e. Using an unauthorised email address to access personal data; and
    f. Leaving paper documents containing personal data in a place accessible to other people.

5. Internal Communication

Reporting a data breach upon discovery

- If any member of our **workforce** suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our **workforce**, a **data processor**, or any other individual) then they must contact the Data Protection Officer ("the DPO") immediately at: Matthew Lantos (Data Protection Officer) dpo.lantos@bsp.london

- The data breach may need to be reported to the ICO, and notified to **data subjects**. This will depend on the risk to **data subjects**. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.
- If it is considered to be necessary to report a data breach to the ICO then the Trust must do so within 72 hours of discovery of the breach.
- The Trust may also be contractually required to notify other organisations of the breach within a period following discovery.
- It is therefore critically important that whenever a member of our **workforce** suspects that a data breach has occurred, this is reported internally to the DPO immediately.
- Members of our **workforce** who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach

- In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation

- The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach, and recovering any **personal data**. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:
    a. remote deactivation of mobile devices where possible;
    b. shutting down IT systems;
    c. contacting individuals to whom the information has been disclosed and asking them to delete the information; and
    d. recovering lost data.

Breach investigation

- When the Trust has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.
- Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:
    a. what data/systems were accessed;
    b. how the access occurred;
    c. how to fix vulnerabilities in the compromised processes or systems;
    d. how to address failings in controls or processes.
- Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

Breach analysis*:*

- In order to determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform the Trust as to whether the data breach should be reported to the ICO and notified to **data subjects**, it is necessary to analyse the nature of the data breach.

- Such an analysis must include:
    a. the type and volume of **personal data** which was involved in the data breach;
    b. whether any **special category personal data** was involved;
    c. the likelihood of the **personal data** being accessed by unauthorised third parties;
    d. the security in place in relation to the **personal data**, including whether it was encrypted;
    e. the risks of damage or distress to the **data subject**.
- The breach notification form annexed to this policy must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of the Trust in deciding whether or not to report the breach.

6. External communication

All external communication is to be managed and overseen by the DPO and/or Headteacher.

Law Enforcement

- The DPO and/or head teacher will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.
- DPO and/or head teacher shall coordinate communications with any law enforcement agency.

Other organisations

- If the data breach involves **personal data** which we process on behalf of other organisations, then we may be contractually required to notify them of the data breach.
- The Trust will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

- If Trust is the **data controller** in relation to the **personal data** involved in the data breach, which will be the position in most cases, then the Trust has 72 hours to notify the ICO if the data breach is determined to be notifiable.
- A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:
    a. the type and volume of **personal data** which was involved in the data breach;
    b. whether any **special category personal data** was involved;
    c. the likelihood of the **personal data** being accessed by unauthorised third parties;
    d. the security in place in relation to the **personal data**, including whether it was encrypted;
    e. the risks of damage or distress to the **data subject**.
- If a notification to the ICO is required, then see part 7 of this policy below.

Other supervisory authorities

- If the data breach occurred in another country or involves data relating to data subjects from different countries, then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

- When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects** then the **data subject** must be notified without undue delay. This will be informed by the investigation of the breach by the Trust.

- The communication will be coordinated by the DPO and will include at least the following information:
    a. a description in clear and plain language of the nature of the data breach;
    b. the name and contact details of the DPO;
    c. the likely consequences of the data breach;
    d. the measures taken or proposed to be taken by Trust to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.
- There is no legal requirement to notify any individual if any of the following conditions are met:
    a. appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);
    b. measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
    c. it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.
- For any data breach, the ICO may mandate that communication is issued to **data subjects**, in which case such communication must be issued.

Press

- Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.
- All press enquiries shall be directed to reception@whtc.co.uk

7. Producing an ICO Breach Notification Report

- All members of our **workforce** are responsible for sharing all information relating to a data breach with the DPO.
- The DPO will provide a Breach Notification Report Form which must be completed in as much detail as possible should be provided.
- The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.
- If any member of our **workforce** is unable to provide information when requested by the DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.
- In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.
- The ICO requires that the Trust send the completed Breach Notification Form to casework@ico.org.uk , with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

8. Evaluation and response

- Reporting is not the final step in relation to a data breach. The Trust will seek to learn from any data breach.
- Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our **workforce** to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

APPENDIX 6 - RETENTION SCHEDULE

Basic file description		Data Protection issues	Statutory Provision	Retention Period [Operational]	**Action at the end of the administrative life of the record**
1. Management of the School This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.					
1.1 Governing Body					
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of.	SECURE DISPOSAL
1.1.2	Minutes, reports and papers of Governing Body meetings - Principal Set (signed)	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
1.1.3	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.4	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.5	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.6	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 6 years	SECURE DISPOSAL
1.1.7	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date of proposal accepted or declined + 3 years	SECURE DISPOSAL

1.2 Headteacher and Senior Management Team					
1.2.1	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies, including correspondence.	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.2	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL
1.3 Admissions Process					
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Mandatory requirements and statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Mandatory requirements and statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Mandatory requirements and statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School attendance: guidance for schools	Every entry in the admission register must be preserved for a period of 3 years after the date on which the entry was made and Review	REVIEW
1.3.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year then Review	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Mandatory requirements and statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels	Current year + 1 year then Review	SECURE DISPOSAL
1.3.7	Supplementary Information form including additional information such as religion, medical conditions, etc.	Yes			
	For successful admissions SECURE DISPOSAL			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process is completed	SECURE DISPOSAL
	Supplementary Information form including additional information such as religion, medical conditions, etc.	Yes			

1.4 Operational Administration					
1.4.1	General file series	No		Current year + 1 year then Review	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 1 year then Review	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	Yes		Current year + 1 year then Review	SECURE DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
	Visitors' Books and Signing in Sheets	Yes		Current year + 3 years then REVIEW	SECURE DISPOSAL
2. Human Resources This section deals with all matters of Human Resources management within the school.					
2.1 Recruitment					
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personnel file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.2 Operational Staff Management					
2.2.1	Staff Personnel File	Yes	Limitation Act 1980 (Section 2)	Termination of employment + 6 years	SECURE DISPOSAL
2.2.2	Annual appraisal/ assessment records	Yes		Current year + 3 years	SECURE DISPOSAL
2.3 Management of Disciplinary and Grievance Processes					
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Yes	Keeping children safe in education Statutory guidance for schools and colleges Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW.	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	Oral warning			Date of warning + 6 years	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
	1st written warning			Date of warning + 6 years	
	Final Written Warning			Date of warning + 6 years	
	Case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety					
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/ injury at work	Yes		Date of incident + 12 years In the case of serious accidents, a further retention period will need to be applied	SECURE DISPOSAL
2.4.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		SECURE DISPOSAL
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.5 Payroll and Pensions					
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL
3. Financial Management of the School This section deals with all aspects of the financial management of the school including the administration of school meals.					
3.1 Risk Management and Insurance					
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
3.2 Asset Management					
3.2.1	Inventories of furniture and Equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3 Accounts and Statements including Budget Management					
3.3.1	Annual Accounts	No		Current year + 6 years	SECURE DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.4	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.5	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL
3.4 Contract Management					
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
3.5 School Fund					
3.5.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL
3.6 School Meals Management					
3.6.1	Free School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

4. Property Management This section covers the management of buildings and property					
4.1 Property Management					
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL
4.2 School Meals Management					
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL
5. Pupil Management This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.					
5.1 Pupil's Educational Record					
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 (SI 2005 No. 1437)		

	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school, the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes		Date of Birth of the pupil + 25 years	SECURE DISPOSAL
	Public			This information should be added to the pupil file	
5.1.3	Child Protection information held on pupil file	Yes	Keeping children safe in education Statutory guidance for schools and colleges Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files	Yes	Keeping children safe in education Statutory guidance for schools and colleges Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 (SI 2005 No. 1437)		

	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school, the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes		Date of Birth of the pupil + 25 years	SECURE DISPOSAL
	Public			This information should be added to the pupil file	
5.1.3	Child Protection information held on pupil file	Yes	Keeping children safe in education Statutory guidance for schools and colleges Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files	Yes	Keeping children safe in education Statutory guidance for schools and colleges Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded
Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.					

5.2 Attendance					
5.2.1	Attendance Registers	Yes	School attendance: guidance for schools	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorised absence		Education Act 1996 (Section 7)	Current academic year + 2 years	SECURE DISPOSAL
5.3 Special Educational Needs					
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years	SECURE DISPOSAL unless the document is subject to a legal hold
6. Curriculum Management					
6.1 Statistics and Management Information					
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	Examination Papers (All)			The examination papers should be kept until any appeals/validation process is complete, unless exam boards require otherwise.	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 3 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 3 years	SECURE DISPOSAL
6.2 Implementation of Curriculum					
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	

6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year. Otherwise it should be destroyed unless used for publicity, displays, etc.	SECURE DISPOSAL
7. Curricular Activities					
7.1 Educational Visits outside the Classroom					
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years. The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	
8. Central Government and Local Authority **This section covers records created in the course of interaction between the school and the local authority.**					
8.1 Local Authority					
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL
8.2 Central Government					
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

APPENDIX 7 - PUPIL PRIVACY NOTICE

Why are we giving this to you?
As your school we need to use information about you. We do this for a number of reasons. This form tells you what information we use about you and why we use it. It is very important that information about you is kept safe. We explain below how the school keeps your information safe.

If you want to know anything about what we do with information about you then please ask your teacher, or speak to your parents/guardians and ask them to contact the school. The school wants you to feel free to raise any questions at all.

We also have a person called the Data Protection Officer at the school. They can answer any questions you have about what the school does with your information. If you or your parents/ guardians want to speak to them, then you can do at: Matthew Lantos dpo.lantos@bsp.london

Policy Statement
All schools within the Wembley Multi Academy Trust (the "Trust") are committed to ensuring data about you is processed in a fair and transparent way. During your time with us, we will use information that we gather in relation to you for various purposes. Information that we hold in relation to you is known as "personal data". This will include data that we obtain from you directly and data about you which we obtain from other people and organisations. We might also need to continue to hold your personal data for a period of time after you have left the school. Anything that we do with your personal data is known as "processing".

This document sets out what personal data we will hold about you, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

What information do we use about you?
We will collect, hold, share and otherwise use information about you set out in the boxes below:

• Name	• Telephone and email contact details	• Date of Birth
• Address	• Assessment information	• Details of previous/future schools
• Unique pupil number	• Behavioural information	• Language(s)
• Nationality	• Country of birth	• Eligibility for free school meals
• Photographs	• Attendance information	• CCTV images

We will also collect, hold, share and otherwise use some information about you which is special "special category personal data" and we will take extra care to make sure that this is kept safe:

• Racial or ethnic origin	• Religious beliefs	• Special educational needs and disability information
• Medical / health information	• Genetic and biometric data	• Information relating to keeping you safe
• Sexual life	• Sexual orientation	• Dietary requirements

Where do we get this information from?
We get this information from:

- You
- Your parents/guardians, and other children's parents/guardians
- Teachers and other staff
- People from other organisations, like doctors or the local authority for example

Why do we use this information?
We use this information for lots of reasons, including:

- To make sure that we give you a good education and to support you through this
- To make sure that we are able to address and support any educational, health or social needs you may have
- To make sure everyone is treated fairly and equally
- To keep you and everyone at the school safe and secure
- To deal with emergencies involving you
- To celebrate your achievements
- To provide reports and additional information to your parents/carers

Some of these things we have to do by law. Other things we do because we need to so that we can run the school.

Sometimes we need permission to use your information. This includes taking pictures or videos of you to be used on our website or in the newspaper. Before we do these things, we will ask you or if necessary your parent/carer for permission.

Why do we use special category personal data?
We may need to use the information about you which is special (mentioned above) where there is a specific interest to do so for example health and social care purposes or to provide you with equal opportunities and treatment. We will also use this information where you have given us permission to do so.
There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests and where you are unable to provide your consent.

How long will we hold information in relation to our pupils?
We will hold information relating to you only for as long as necessary. How long we need to hold on to any information will depend on the type of information. Where you change school, we will usually pass your information to your new school.

Who will we share pupil information with?
We may share information about you with:

- Other schools or educational institutions you may attend or require support from Local Authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes
- The Department for Education and/ or ESFA as required by the law
- Contractors, to enable them to provide an effective service to the school, such as school meal providers, external tutors or access to online learning.

Keeping this information safe
It is very important that only people who need to use your information can see it. The school keeps your information safe by:

- Storing all data in a safe and secure environment. This applies to both paper copies and electronic data
- Only allowing access to your data to those that legitimately need it.

Your rights in relation to your information
You can ask to see the information we hold about you. If you wish to do this, you should contact your Year Leader in the first instance who will guide you in how to go about your request.

You also have the right to:

- Ask us to stop doing certain things with your information in some cases
- Have inaccurate or incomplete information about you amended
- Ask that decisions about you are not made using automatic systems
- Claim against the school in certain circumstances where you have suffered as a result of the school breaching your data protection rights

If you feel it necessary to do any of the above, you can speak with your Year Leader in the first instance. The school does not have to meet all of your requests and we will let you know where we are unable to do so.

Concerns
If you are concerned about how we are using your personal data then you can speak with Matthew Lantos dpo.lantos@bsp.london, or if necessary you or your parent/carer can contact an outside agency - the Information Commissioner's Office who could also help at https://ico.org.uk/concerns/

APPENDIX 8 - PARENT / CARER PRIVACY NOTICE

Policy Statement
Wembley Multi-Academy Trust (the "Trust") is committed to ensuring data about you and your child is processed in a fair and transparent way. During your child's time with us, we will gather and use information relating to you. Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from you directly and data about you that we obtain from other people and organisations. We might also need to continue to hold your personal data for a period of time after your child has left the Trust. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will hold about you, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

What information do we process in relation to you?
We will collect, hold, share and otherwise use the following information about you:

- personal information (such as name, address, home and mobile numbers, personal email address, emergency contact details and relationship marital status)
- financial details (such as bank account or credit card details), and other financial details such as eligibility for free school meals or other financial assistance
- CCTV footage and images obtained when you attend the Trust site
- your relationship to your child, including any Court orders that may be in place

We will also use special categories of data such as gender, age, ethnic group, sex or sexual orientation, religious or similar beliefs, information about health, genetic information and biometric data. These types of personal data are subject to additional requirements.

Where do we get your personal data from?
We will obtain an amount of your personal data from you, by way of information gathering exercises at appropriate times such as when your child joins the Trust and when you attend the Trust site and are captured by our CCTV system.

We may also obtain information about you from other sources. This might include information from the local authorities, including schools, or other professionals or bodies, including a Court, which might raise concerns in relation to your child.

Why do we use your personal data?
We will process your personal data for the following reasons:

1. Where we are required by law, including:
    - To provide reports and other information required by law in relation to the performance of your child
    - To raise or address any concerns about safeguarding
    - To the Government agencies including the police
    - To obtain relevant funding for the school
    - To provide or obtain additional services including advice and/or support for your family

2. Where the law otherwise allows us to process the personal data as part of our functions as a Trustor we are carrying out a task in the public interest, including:

   - To confirm your identity
   - To communicate matters relating to the Trust to you
   - To safeguard you, our pupils and other individuals
   - To enable payments to be made by you to the Trust
   - To ensure the safety of individuals on the Trust site
   - To aid in the prevention and detection of crime on the Trust site

3. Where we otherwise have your consent
   Whilst the majority of processing of personal data we hold about you will not require your consent, we will inform you if your consent is required and seek that consent before any processing takes place.

Why do we use special category personal data?
We may process special category personal data in relation to you for the following reasons:

1. Where the processing is necessary for reasons of substantial public interest, including for purposes of equality of opportunity and treatment, where this is in accordance with our Data Protection Policy.
2. Where the processing is necessary in order to ensure your health and safety on the Trust site, including making reasonable adjustments for any disabilities you may have.
3. Where we otherwise have your explicit written consent.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests of those of your child, and where it is not possible to seek your consent.

Failure to provide this information
If you fail to provide information to us we may be prevented from complying with our legal obligations.

How long will we hold your personal data for?
We will hold your personal data only for as long as necessary. How long we need to hold on to any information will depend on the type of information. For further detail please see our Retention and Destruction Policy.

Who will we share your personal data with?
We routinely share information about you with:

- Local authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes
- The Department for Education and/or the Education and Skills Funding Agency, in compliance with legal obligations of the school to provide information about students and parents as part of statutory data collections
- Contractors, such as payment processing providers to enable payments to be made by you to the Trust

The Department for Education may share information that we are required to provide to them with other organisations. For further information about the Department's data sharing process, please visit: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data.
Contact details for the Department can be found at https://www.gov.uk/contact-dfe.
Local authorities may share information that we are required to provide to them with other organisations. For further information about Brent local authority's data sharing process, please visit: https://www.brent.gov.uk

Contact details for Brent local authority can be found at https://www.brent.gov.uk

APPENDIX 9 - WORKFORCE PRIVACY NOTICE

Policy Statement
Wembley Multi-Academy Trust (the "Trust") is committed to ensuring data about you is processed in a fair and transparent way. During an individual's time with us, we will use information that we gather in relation to them for various purposes. Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from the individual directly and data about the individual that we obtain from other people and organisations. We might also need to continue to hold an individual's personal data for a period of time after they have left the school. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will hold about our workforce, why we process that data, who we share this information with, and the rights of individuals in relation to their personal data processed by us.

What information do we process in relation to our workforce?
We will collect, hold, share or otherwise use the following information about our workforce:

- personal information (such as name, address, home and mobile numbers, personal email address, employee or teacher number, national insurance number, and emergency contact details)
- contract information (such as start dates, hours worked, post, roles and salary information, bank/building society details)
- work absence information (such as number of absences and reasons (including information regarding physical and/or mental health), holiday records)
- qualifications / training courses attended and, where relevant, subjects taught (such as training record)
- performance information (such as appraisals and performance reviews, performance measures including performance management/improvement plans, disciplinary or grievance records)
- other information (such as pension arrangements (and all information included in these necessary to administer them), time and attendance records, information in applications made for other posts within the school, criminal records information (including the results of Disclosure and Barring Service (DBS) checks), details in references the school receives or provides to other organisations, CCTV footage and images).

We will also use special categories of data including such as gender, age, ethnic group, sex or sexual orientation, religious or similar beliefs, political opinions, trade union membership, information about health, genetic information and biometric data. These types of personal data are subject to additional requirements.

Where do we get information from about our workforce?
A lot of the information we have about our workforce comes from the individuals themselves. However, we may also obtain information from tax and regulatory authorities such as HMRC, previous employers, your trade union, the DBS, our insurance benefit administrators, consultants and other professionals we may engage, recruitment or vetting agencies, other members of staff, students or their parents, and publicly available resources including online sources. In addition, we may obtain information from automated monitoring of our websites and other technical systems such as our computer networks and systems, CCTV and access control systems, communications systems, remote access systems, email and instant messaging systems, intranet and internet facilities, telephones, voicemail and mobile phone records.

Why do we use this information?

We will process the personal data of our workforce for the following reasons:

1. Where we are required by law, including:
   - To comply with the law regarding data sharing (see further below)
   - To comply with specific employment law requirements, including our obligations as an employer under employment protection and health and safety legislation, and under statutory codes of practice such as those issued by ACAS
   - To comply with legal requirements in relation to equalities and non-discrimination
   - Any other relevant legislation where we are required to process your data or are required to by other bodies (e.g. police service, a Court of Law, etc.).

2. Where we are required by any contract with our workforce, such as employment contracts, including:
   - To make payments to our workforce, such as salary payments
   - To deduct tax and National Insurance contributions
   - To make a decision about recruitment
   - To check individuals are legally entitled to work in the UK
   - Administering employment contracts
   - Conducting performance reviews
   - Making decisions about salary and compensation
   - Liaising with pension providers
   - Providing any further employment benefits, such as access to BUPA Health Care

3. Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest, including:
   - To enable the development of a comprehensive picture of the workforce and how it is deployed
   - To inform the development of recruitment and retention policies
   - To safeguard our pupils and other individuals
   - To ensure safe working practices
   - In the interests of ensuring equal opportunities and treatment

4. Where we otherwise have the consent of the individual
   Whilst the majority of processing of personal data of our workforce will not require consent, we will inform individuals if their consent is required and seek that consent before any processing takes place. Due to the imbalance of power in an employee to employer relationship, it is generally thought that although consent may be implied it cannot truly be freely given. So, consent is not necessarily the most appropriate basis to rely upon as an employer.

Why do we use special category personal data?

We may process special category personal data of our workforce for the following reasons:

1. To carry out our legal obligations in relation to employment law, where this is in accordance with our Data Protection Policy
2. Where the processing is necessary for reasons of substantial public interest, including for purposes of equality of opportunity and treatment, where this is in accordance with our Data Protection Policy.
3. For the purposes of preventative or occupational medicine in order to assess an individual's working capacity and/ or the need for reasonable adjustments.
4. Where we otherwise have an individual's explicit written consent – subject to the restriction set out above on the use of consent in an employment relationship.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests and where you are unable to provide your consent.

Failure to provide this information
If our workforce fail to provide information to us then this may result in us being unable to perform the employment contract, or we may be prevented from complying with our legal obligations.

How long will we hold information in relation to our workforce?
We will hold information relating to our workforce only for as long as necessary. How long we need to hold on to any information will depend on the type of information. For further details, please see our Retention and Destruction Policy.

Who will we share information with about our workforce?
We routinely share information about our workforce with:

- The Department for Education and/or the ESFA, in compliance with legal obligations of the school to provide information about our workforce as part of statutory data collections
- Contractors, such as payroll providers, to enable them to provide an effective service to the school, government agencies such as HMRC and DWP regarding tax payments and benefits, teachers pensions, and other government and non-governmental agencies.
- Our professional advisors including legal and HR consultants

The Department for Education may share information that we are required to provide to them with other organisations. For further information about the Department's data sharing process, please visit: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data.
Contact details for the Department can be found at https://www.gov.uk/contact-dfe.

Rights of our workforce in relation to their personal data
All of our workforce have the right to request access to personal data that we hold about them. To make a request for access to their personal data, individuals should contact their Leadership Line Manager in the first instance.

Please also refer to our Data Protection Policy on our website for further details on making requests for access to workforce information.
Individuals also have the right, in certain circumstances, to:

- Restrict processing of their personal data
- Have inaccurate or incomplete personal data about them rectified
- Object to the making of decisions about them taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of their data protection rights

If an individual wants to exercise any of these rights then they should contact their Leadership Line Manager in the first instance. The law does not oblige the school to comply with all requests. If the school does not intend to comply with the request, then the individual will be notified of the reasons why in writing.

Concerns
If an individual has any concerns about how we are using their personal data, then we ask that they contact our Data Protection Officer in the first instance. However, an individual can contact the Information Commissioner's Office should they consider this to be necessary, at https://ico.org.uk/concerns/.

Contact
If you would like to discuss anything in this privacy notice, please contact: Matthew Lantos dpo.lantos@bsp.london

Your rights in relation to your personal data held by us
We will not process the biometric data of a pupil (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
b) no parent has consented in writing to the processing; or
c) a parent has objected in writing to such processing, even if another parent has given written consent.

You have the right to request access to personal data that we hold about you, subject to a number of exceptions. To make a request for access to your personal data, you should contact: Matthew Lantos dpo.lantos@bsp.london

Please also refer to our Data Protection Policy for further details on making requests for access to your personal data.

You also have the right, in certain circumstances, to:

- Restrict processing of your personal data
- Have inaccurate or incomplete personal data about you rectified
- Object to the making of decisions about you taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of your data protection rights

If you want to exercise any of these rights then you should contact reception@whtc.co.uk. The law does not oblige the Trust to comply with all requests. If the Trust does not intend to comply with the request, then you will be notified of the reasons why in writing.

Concerns
If you have any concerns about how we are using your personal data, then we ask that you contact our Data Protection Officer in the first instance. However, an individual can contact the Information Commissioner's Office should you consider this to be necessary, at https://ico.org.uk/concerns/

Contact
If you would like to discuss anything in this privacy notice, please contact: Matthew Lantos dpo.lantos@bsp.london

APPENDIX 10 - RECRUITMENT PRIVACY NOTICE

Policy Statement
Wembley Multi-Academy Trust (the "Trust") is committed to ensuring data about you is processed in a fair and transparent way. As part of your application to join us, we will gather and use information relating to you.

Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from you directly and data about you that we obtain from other people and organisations. We might also need to continue to hold an individual's personal data for a period of time after the recruitment process, even if you are unsuccessful. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will gather and hold about individuals who apply for a position with us, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

What information do we process during your application process?
We may collect, hold, share and otherwise use the following information about you during your application process.
Up to and including shortlisting stage:

- your name and contact details (i.e. address, home and mobile phone numbers, email address);
- details of your qualifications, training, experience, duties, employment history (including job titles, salary, relevant dates and working hours), details of driving licence (if relevant for role), membership of professional bodies and interests;
- your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;
- information regarding your criminal record;
- details of your referees;
- whether you are related to any member of our workforce;
- details of any support or assistance you may need to assist you at the interview because of a disability; and
- any online presence and information publicly available will be scrutinised.

Following shortlisting stage, and prior to making a final decision

- information about your previous academic and/or employment history, including details of any conduct, grievance or performance issues, appraisals, time and attendance, from references obtained about you from previous employers and/or education providers;
- any online presence and information publicly available will be scrutinised;
- confirmation of your academic and professional qualifications (including seeing a copy of certificates);
- information via the DBS process, regarding your criminal record, in criminal records certificates (CRCs) and enhanced criminal records certificates (ECRCs), whether you are barred from working in regulated activity;
- your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- medical check to indicate fitness to work;
- a copy of your driving licence (or other appropriate documentation as listed on the Home Office list);
- if you are a teacher, we will check the National College of Teaching and Leadership ("NCTL") Teachers Services about your teacher status, whether you are subject to a prohibition from teaching order and any other relevant checks (for example Section 128 direction for management posts and EEA teacher sanctions); and
- equal opportunities' monitoring data.

You are required (by law or in order to enter into your contract of employment) to provide the categories of information marked (*) above to us to enable us to verify your right to work and suitability for the position. Without providing us with this information, or if the information is not satisfactory, then we will not be able to proceed with any offer of employment.

If you are employed by us, the information we collect may be included on our Single Central Record.

Where do we get information from about during your application process?
Depending on the position that you have applied for, we may collect this information from you, your referees (details of whom you will have provided), your education provider, any relevant professional body, the Disclosure and Barring Service (DBS), NCTL and the Home Office, during the recruitment process.

Why do we use this information?
We will process your personal data during your application process for the purpose of complying with legal obligations, carrying out tasks which are in the public interest, and taking steps with a view to entering into an employment contract with you. This includes:

- to assess your suitability for the role you are applying for;
- to take steps to enter into a contract with you;
- to check that you are eligible to work in the United Kingdom or that you are not prohibited from teaching; and
- so that we are able to monitor applications for posts in the Trust to ensure that we are fulfilling our obligations under the public sector equality duty under the Equality Act 2010.

How long will we hold information in relation to your application?
We will hold information relating to your application only for as long as necessary. If you are successful, then how long we need to hold on to any information will depend on type of information. For further detail please see our Retention and Destruction Policy.

If you are unsuccessful we will hold your personal data only until the end of the academic year, after which time it is securely deleted.

Who will we share information with about your application?
We will not share information gathered during your application process with third parties, other than professional advisors such as legal as HR advisors, or if we are otherwise required to.

Rights in relation to your personal data
All individuals have the right to request access to personal data that we hold about them. To make a request for access to their personal data, individuals should contact: reception@whtc.co.uk

Please also refer to our Data Protection Policy available on our website for further details on making requests for access to personal data.
Individuals also have the right, in certain circumstances, to:

- Restrict processing of their personal data
- Have inaccurate or incomplete personal data about them rectified
- Object to the making of decisions about them taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of their data protection rights

If an individual wants to exercise any of these rights then they should contact reception@whtc.co.uk . The law does not oblige the school to comply with all requests. If the school does not intend to comply with the request, then the individual will be notified of the reasons why in writing.

Concerns

If an individual has any concerns about how we are using their personal data, then we ask that they contact our Data Protection Officer in the first instance. However, an individual can contact the Information Commissioner's Office should they consider this to be necessary, at https://ico.org.uk/concerns/.

Contact

If you would like to discuss anything in this privacy notice, please contact: Matthew Lantos dpo.lantos@bsp.london