



Teaching London

Data Protection Policy Teaching London: LDBS SCITT

Policy agreed: September 2022
Next review: September 2023

Contents

| | |
|---|----|
| 1. Aims | 3 |
| 2. Legislation and guidance | 3 |
| 3. Definitions | 3 |
| 4. The data controller | 4 |
| 5. Roles and responsibilities | 4 |
| 6. The Data protection principles | 6 |
| 7. Collecting personal data | 6 |
| 8. Sharing personal data | 7 |
| 9. Individuals Data Protection Rights | 8 |
| 10. Closed Circuit Television (CCTV) | 10 |
| 11. Photographs and videos | 10 |
| 12. Data protection by design and default | 11 |
| 13. Data security and storage of records | 11 |
| 14. Disposal of records | 12 |
| 15. Personal data breaches | 12 |
| 16. Monitoring arrangements | 12 |
| 17. Links with other policies | 12 |

1. Aims

Teaching London aims to ensure that all personal data collected, stored, processed or destroyed about any natural person, whether they be a member of staff, trainee, visitor, contractor, consultant or other individual, is done so in accordance with the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, collected, stored, processed and destroyed by Teaching London, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated.

2. Legislation and guidance

This policy meets the current requirements of current Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and DPA 2018. It is also based on the information provided by the Article 29 Working Party.

It also meets the requirements of the Protection of Freedoms Act 2012, the ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information.

3. Definitions

| <u>Term</u> | <u>Definition</u> |
|------------------------|---|
| Data controller | The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| Data processor | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, following the controller's instruction. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Consent | Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. |
| Personal data | Any information relating to an identified or identifiable natural person ('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 <ul style="list-style-type: none">• 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. |

Special categories of personal data

Personal data which is more sensitive and so needs more protection, including Information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation
- history of offences, convictions or cautions *

* Note: Whilst criminal offences are not listed as special category data, within this policy they are regarded as such in acknowledgment of the extra care which is needed with this data set.

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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 can be automated or manual.

Data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Teaching London processes personal data relating to trainees, staff, visitors and others, and therefore is a data controller and a data processor.

Teaching London is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The registration number is ZA826619

5. Roles and responsibilities

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

5.1 Programme Director

The Programme Director has overall responsibility for ensuring that Teaching London complies with all relevant data protection obligations.

5.2 Data Protection Officer

Teaching London has appointed Grow Education Partners Ltd as its Data Protection Officer (DPO). The responsible contact is Claire Mehegan, Claire.mehegan@london.anglican.org

They are responsible for overseeing the implementation of this policy in the first instance, before reviewing our compliance with data protection law, and developing related policies and guidelines where applicable.

Upon request the DPO can provide an annual report of Teaching London's compliance and risk issues directly to the Programme Director and will report their advice and recommendations on data protection issues.

The DPO is a named point of contact for all data subjects whose data Teaching London processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description and the SLA for Service.

5.3 Representative of the data controller

Saskia Rossi, Business Manager, acts as the representative of the data controller on a day-to-day basis.

5.4 All staff and trainees

Staff and trainees (regardless of role) are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy (and the policies of the schools in which they are training)
- Informing Teaching London of any changes to their personal data, e.g. a change of address, telephone number, or bank details
- Reporting a Data Breach, Data Right Request, or Freedom of Information Request
- Contacting the DPO:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

Data Protection is based on seven principles that Teaching London must comply with.

These are that data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

The Accountability principle ties these all together by requiring an organisation to take responsibility for complying with the other six principles, including having appropriate measures and records in place to be able to demonstrate compliance.

This policy sets out how Teaching London aims to comply with these key principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

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

For special categories of personal data, we will also meet one of the special category conditions for processing which are set under data protection law.

These are where:

- The individual has **given explicit consent**
- It is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** of a data controller or of a data subject
- It is necessary to protect the **vital interests** of the data subject
- Processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim**

- The personal data has **manifestly been made public** by the data subject
- There is the **establishment, exercise or defence of a legal claim**
- There are reasons of **public interest** in the area of **public health**
- Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment);
- There are **archiving** purposes in the **public interest**.

Where we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice.

These privacy notices can be found in a location accessible and relevant to the data subjects

- Trainees: <https://www.teachinglondon.org/privacy-policies/>
- Employees: <https://www.teachinglondon.org/privacy-policies/>
- Job Applicants: <https://www.teachinglondon.org/privacy-policies/>
- Visitors: <https://www.teachinglondon.org/privacy-policies/>

Additional Copies of the Privacy Notices are available on request by contacting **admin@teachinglondon.org**

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data, in our privacy notices.

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

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

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When personal data is longer required, staff must ensure it is deleted. This will be done in accordance with Teaching London document retention policy, which states how long particular documents should be kept, and how they should be destroyed.

Copies of the Document Retention Policy can be obtained by contacting **admin@teachinglondon.org**

8. Sharing personal data

In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to situations where:

- There is an issue that puts the safety of a staff member, trainee or school pupil at risk
- We need to liaise with other agencies or services – we may seek consent when appropriate before doing this, where possible
- Our suppliers or contractors need data to enable us to provide services to our staff and trainees – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law and have satisfactory security measures in place
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies when required to do so, for reasons which include but are not limited to:

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects trainees, staff or others.

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

9. Individuals' Data Protection Rights

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to access personal information that an organisation holds about them. This includes:

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

While Teaching London will comply with Data Protection legislation in dealing with all subject access requests submitted in any format, individuals are asked to preferably submit their request by letter, email or fax addressed or marked for the attention of the **Saskia Rossi**.

Email: admin@teachinglondon.org

Post: 2 West End Lane, London, NW6 4NT

They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the **Saskia Rossi**.

9.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification from the list below:
 - passport
 - driving licence
 - utility bill with the current address
 - Birth / Marriage certificate
 - P45/P60
 - credit card or mortgage statement.
- May contact the individual via phone to confirm the request was made by them
- Will respond without delay and within the required regulatory timeframe.
- Will provide the information free of charge (unless the request is found to be onerous, excessive or unfounded). Any fee charged will be reasonable and will only account for the administrative costs incurred while complying with the request
- May tell the individual we will comply within 3 months of receipt of their request, where requests are complex or numerous. We will inform the individual of this as soon as possible and explain why the extension is necessary.

We will not disclose information if it:

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

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

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

In the event we refuse a request, we will tell the individual why and tell them they have the right to refer a complaint to the ICO.

9.3 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time [NB: this only relates to tasks for which Teaching London relies on consent to process the data]
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling [decisions taken with no human involvement, that might negatively affect them]
- Request the cessation of any processing that is likely to cause damage or distress
- Be notified of a data breach [in certain circumstances]
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format [in certain circumstances]

Individuals have the right to exercise these rights at any point These should be submitted to **Saskia Rossi**. If staff receive such a request, they must immediately forward it onwards.

10. Closed Circuit Television (CCTV)

We use CCTV in various locations around Teaching London's premises for the following purposes:

- To provide a safe and secure environment for staff, trainees and visitors
- To protect buildings and assets
- To assist in the prevention and detection of criminal activity
- To assist law enforcement agencies in apprehending suspected offenders.

We adhere to the ICO's code of practice for the use of CCTV and provide training to relevant staff in its use.

We do not need to ask individuals' permission to use CCTV, but in most instances we make it clear where individuals are being recorded, with security cameras that are clearly visible and accompanied by prominent signs explaining that CCTV is in use, Where the location of cameras is not clear, directions will be given on how further information can be sought.

The full CCTV policy can be found on the **Teaching London website**. Any enquiries about the CCTV system should be directed to **Christopher Woolridge**.

11. Photographs and videos

As part of our activities, we may take photographs and record images of individuals.

The use of photographs includes but is not limited to:

- Within our premises on notice boards and in magazines, brochures, newsletters and prospectuses
- Outside our premises by external agencies and partners such as local and national newspapers and local and national campaigns with which we are involved
- Online on our website or social media pages.

We will obtain consent from the responsible individuals in order to use photos and images. When doing so we will clearly explain how the photograph and/or video will be collected and used when obtaining consent.

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

You can withdraw consent by ***sending a written request to admin@teachinglondon.org***

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data collection and processing activities. These include, but are not limited to the following organisational and technical measures:

- Appointing a suitably qualified DPO and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection regulations
- Completing data privacy impact assessments where Teaching London's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies or processing tools. Advice and guidance will be sought from the DPO
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regular training for Teaching London workforce on data protection law, this policy and any related policies and any other data protection matters. Records of attendance to ensure that all data handlers receive appropriate training
- Periodic audits to monitor and review our privacy measures and make sure we are compliant with legislation and our own policies
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our Data Protection Officer and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold; maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

13. Data security and storage of records

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

In particular our organisational and technical measures include:

- Paper-based records and portable electronic devices such as laptops, tablets and hard drives that contain personal data will be kept under lock and key when not in use
- Sensitive personal data will not be left out on view when not in use unless there is a compelling lawful basis to do so (e.g. display of allergy information in case of a medical emergency)
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff and trainees are reminded to change their passwords at regular intervals

- Staff or trainees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see ***E- safety policy and Email Security and Etiquette Guidance for further information***)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will be rectified or updated, unless it is no longer of use and therefore will be disposed of securely.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on Teaching London's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and provide a certificate of destruction.

When records are disposed of as part of the Data Retention schedule this is then recorded on our record of destruction log.

15. Personal data breaches

Teaching London will make all reasonable endeavours to prevent personal data breaches.

All potential or confirmed data breach incidents should be reported to the ***Saskia Rossi*** who will record them in Teaching London's data breach log.

Logged incidents will be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required.

Where appropriate, we will report the data breach to the ICO and affected data subjects within 72 hours.

The full procedure is set out in Teaching London Breach Management Policy, which can be found on the **Teaching London website**.

Examples of a data protection breach include but are not limited to:

- Personal data being left unattended in a meeting room or shared area
- Information relating to a trainee or staff member being sent to the wrong person
- Safeguarding information being made available to an unauthorised person
- The theft of a laptop containing non-encrypted personal data.

16. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy as part of the general auditing and compliance work, they carry out.

They will work with ***Saskia Rossi*** to ensure that this policy remains contemporaneous and appropriate.

This policy will be reviewed annually, and changes recommended when appropriate. The Programme Director will be asked to sign off the policy review and any necessary changes.

17. Links with other policies

This data protection policy is linked to our:

- Freedom of Information request procedure
- E-Safety Policy
- Email Security and Etiquette Guidance
- Data Retention Policy and Schedule
- Breach Management Policy
- Safeguarding, Prevent and Child Protection Policy
- CCTV Policy