



Data Protection Policy

Last Reviewed: September 2020
Next Review Due: September 2021
Reviewed By: Emily Maskell

The London Acorn School Data Protection Policy (in line with GDPR 2018)

The London Acorn School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with (GDPR 2018). It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. GDPR is a new EU regulation covering data protection. It came into force on 25 May 2018 and replaces the data Protection Act (1998) and the Electronic Communications Regulations. All UK companies need to be compliant with this legislation, including organisations that host data on behalf of UK companies.

This policy sets out how The London Acorn School processes the personal data of subjects, including the personal data of job applicants and the personal data of our current and personal data of our current and former Directors, Governors, employees, workers, student placements, contractors, consultants, students, parents/carers, suppliers and other third parties.

The London Acorn School is committed to being clear and transparent about how we use personal data and to complying to our data protection regulations. Protecting the confidentiality, security and integrity of the personal data that we process is also of paramount importance to our business operations. This policy is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any contract for services.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and will process data in accordance with this policy, the data legislation and the latest privacy notice.

Responsibility

The London Acorn School has appointed Emily Maskell, School Business Manager, as the person with overall responsibility for data protection compliance within the organisation. Questions about this policy, or requests for further information, should be directed to her. She can be contacted at emily@thelondonacornschoo.co.uk.

Data Protection Principles

Under GDPR there are six enforceable data principles that must be adhered to at all times. These provide that the personal information we hold about you must be:

1. processed fairly, lawfully and in a transparent manner
2. collected only for legitimate purpose that have been clearly explained to you and not further processed in a way that is incompatible to these purposes.
3. adequate, relevant and limited to what is necessary in relation to these purposes.
4. accurate and where necessary, kept up to date;
5. kept in a form which permits your identification for any longer than is necessary for these purposes
6. processed in a way that ensures appropriate security of data.

General Statement

The school is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Types of personal information we collect

Personal data/information is any information from which a person can be directly or indirectly identified, including children in our care. This may include: family details; GP contact details; financial details; education and employment details; goods and services provided.

Additionally, with parent/guardian consent, we will safely and securely record evidence of child(ren) playing and learning at the London Acorn School (i.e. photographs) and

information relating to child development/progress at TLAS purely for the purposes of keeping families updated in the education they are receiving at TLAS.

There are also “special categories “of personal information, and personal information on criminal convictions and offences, which require a higher level of protection because it is of a more sensitive nature. The special categories of personal information comprise information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

The London Acorn School collects, uses and processes a range of personal data for the purposes of:

1. Using the information to comply with our legal obligations.
2. Using information for effective communication (e.g. contact details) for the effective operation of the school.
3. To support all who work for us and the children in our care (including governors and Directors)

The school may also collect data to use and process the following special categories of personal data (as applicable):

- Physical or mental health details (for safeguarding purposes and for which the company needs to make reasonable adjustments).
- Racial or ethnic origin, religious or philosophical beliefs (to respect family beliefs/culture – e.g. food and holidays).
- Criminal convictions and offences (for safer recruitment purposes).

How we collect personal information

We obtain personal information when:

- The London Acorn School receives or send an email.
- Prospective families initially enquire about Little Acorns/ Kindergarten/ school places, events or activities.
- Families register their children for a trial/ permanent place in the school.
- Potential employees/volunteers/governors apply to work with TLAS.
- Staff work at TLAS.
- Governor/Director works with TLAS.

The personal information we hold on any individual has been provided either by that individual and/or where data has been provided by a third party for the purposes of recruitment, the school will only seek to obtain personal information from third parties during the recruitment process once the candidate has been short listed and the candidate has been informed that we are doing so.

Personal data/information may be stored in different places in the Schools IT Management systems, on paper where it is stored securely and in other IT systems such as email.

How we use personal data – our reasons/purposes for processing information

We need all types of personal information listed under “how we collect personal information” primarily to enable us to take steps at your request to enter into a contract with you and to enable us to comply with legal obligations. In some cases, we may also use your personal information where it is necessary to pursue our legitimate interests (or those of a third party) provided that your interests or your fundamental rights and freedoms do not override our interests. Our legitimate interests include: pursuing our business by employing employees, workers and contractors, managing the recruitment process; conducting due diligence on prospective staff and performing effective internal administration.

The purpose for which we collect, hold, process personal information is to enable TLAS to;

- Provide safe, effective education (ensuring the welfare and protection of that child)
- Manage the effective operation of the education we provide and communicate with all service users, employees, governor, directors and those external to the organisation.
- Safely recruit personnel- comply with statutory and/or regulatory requirements and obligations e.g. checking right to work in the UK; comply with the duty to make reasonable adjustments and other disability discrimination obligations.
- Support and manage staff.
- Ensure compliance with statutory rights.
- Ensure effective PR, personnel management and business administration.
- Enable us to establish, exercise or defend possible legal claims.
- Manage our legal/regulatory compliance obligations (Child personal data needs to be kept till a child is 21 years of age; financial accounts need to be retained for 7 years, gift aid forms need to be retained for 7 years; pension details need to be kept for a minimum of 6 years).

Please note that we may process personal information without your consent, in compliance with these rules, where it is required by law. We process information in line with regulatory requirements (e.g. Ofsted, Companies House) and in line with legislation relating to “Working Together to Safeguard Children (2015) Policy (e.g. Protection of Children Act 1989, Children’s Act 2004; Rehabilitation of Offenders Act 1974; Education Act 2011; Counter-Terrorism and Security Act 2015).

We may also occasionally use special categories of personal information, and information about criminal convictions and offences, where it is needed to establish, exercise or defence of legal claims.

Consent- how we seek, obtain and record consent

To ensure that we obtain personal data safely, and in line with data protection compliance, many of our procedures require a signature of consent. (Note- parents/guardians will provide consent for any child in our care who is under 13 years of age).

In order to comply with EYFS and Ofsted legislation/regulation, there is a large amount of data that we must keep hold of. These legal obligations override GDPR and therefore, we do not need consent to collate certain data (e.g. child and parent details must be

kept/recorded for 2 years, accident reports must be kept for 21 years and 3 months, staff records must be kept for 7 years) For existing parents, who joined before 25 May 2018, who have already given consent on enrolment forms, we do not have to gain consent again.

We have reviewed our School communication, including policies and procedures, to ensure where consent is sought that is: freely given, specific, informed, unambiguous, demonstrable (by a statement of clear affirmative action) e.g. Tick boxes, signature, with separate consent sought as required.

Access to personal information

Personal information may be shared internally within the school for the purpose of the recruitment exercise, including with school leadership members (Directors, Head teacher, School Business Manager, IT Staff) if access to your personal information is necessary for the performance of their roles.

The school will not share personal with third parties unless for the purpose of recruitment or child safeguarding or legal advice. We may also need to share your information with a regulator (e.g. Ofsted) or to otherwise comply with the law.

How the school protects personal information

We work hard protect all personal data from unauthorised access and/or disclosure. We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorised access, alteration, disclosure or destruction of your personal or transactional data stored on our website and systems. Personal data information is either managed on secure online systems OR kept safe in secure lockable filing cabinets/offices, where paperwork has been completed.

To protect security of personal information, we limit access to personal information to those employee, workers and other third parties who have a business need to know to perform their job duties and responsibilities. Additionally, we have put in place staff training and internal procedures/controls to try and prevent personal information from being accidentally lost or destroyed or used or accessed in an unauthorised way.

Where your personal data is shared with third parties, we require all third parties to take appropriate technical and organisational security measures to protect personal information and to treat it subject to a duty of confidentiality and in accordance with data protection law.

TLAS also has in place procedures to deal with a suspected data security breach and will notify the Information Commissioners Office (or any other applicable supervisory authority or regulator) of a suspected breach where we are legally required to do so. Please note- we may share your personal information with third parties where it is necessary, as steps in your request to enter into a contract with you, where we need to comply with a legal obligation, or where necessary for our legitimate interests (or those of a third party).

Who the information will be shared with

We work with data compliant registered companies who host and/or process data on TLAS's behalf. For further information about these third-party data processing organisations and their data compliance procedures, please see the following:

DATA PROCESSING ORGANISATIONS:

- For assessment tracking data purposes: Otrack Assessment tracker: <https://secure2otrack.co.uk/privacypolicy.aspx>
- For financial data purposes-XERO, <https://www.xero.com/uk/about/terms/privacy/>
- For staff payroll and Company auditing: DJCA, <https://www.djca.co.uk/privacy-policy/>
- For staff pension: NEST, <https://www.nestpensions.org.uk/schemeweb/nest/nestcorporation/privacy-policy.html>
- For staff training: EDUCARE <https://www.educare.co.uk/privacynotice>
- For staff, volunteers and governors DBS checks- GBC online disclosures
- For company operation (i.e. staff email and work documentation) [Microsoft Office 365 accounts://Microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx](https://Microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx)
- For IT support: Novacore, t.mundy@novacore.co.uk
- For card payment/banking purposes: Stripe, <https://stripe.com/gb/privacy>
- PayPal, <https://www.paypal.com/uk/webapps/mpp/ua/privacy-full>
- For staff Performance Management Standards Tracker: <https://standardstracker.co.uk/privacy-policy>

DATA CONTROL AND PROCESSING ORGANISATIONS:

For Early Years funding/and or child safeguarding protocol: The London Borough of Merton: <https://www.merton.gov.uk/council-and-local-democracy/data-protection-and-freedom-of-information>

Additionally, we occasionally need to share the personal information we process with other organisations, as compliance with our regulatory and legal obligations. What follows is a description of the types of organisations we may need to share some of the personal information we process with, for one or more reasons. Where necessary or required we share information with:

- Family, associates and representatives of the person whose personal data we are processing.
- Healthcare, social and welfare advisors or practitioners.
- Credit reference agencies, debt collection and tracing agencies
- Education, educators and examining bodies.
- Current, past or prospective employers.
- Employment and recruitment agencies.
- Schools.
- Local and central government.
- Persons making an enquiry or complaint.
- Regulatory bodies (Ofsted, Companies House).
- Legal advice/insurance companies.

We will not share any personal information to another party for purposes of marketing. We will only use personal information, where there is no disadvantage to the person to whom it relates

How long does the TLAS keep personal information?

We keep information for as long as it is necessary to fulfil the purposes for which it was collected and processed and to operate the school in accordance with legal requirements, tax and accounting rules. Where your information is no longer required, we will ensure it is disposed of in a secure manner.

For pupil enrolment -The school is legally required to keep child records up to when they reach 21 years of age for the purposes of safeguarding (this includes, and is not restricted to, enrolment form detail, medical/health information, Special Educational Needs (SEN) details, records relating to child safeguarding/child protection, accident and incident records, all records relating to “looked after child” – i.e. the child is fostered/adopted). Additionally, enrolment form details will contain parent/guardian contact details which may also be used for debt collection purposes.

For Staff recruitment purposes- TLAS will generally hold your personal information for six months after the end of the relevant recruitment exercise but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirement for particular data or records and (b) the retention of some types of personal information for up to (six years) to protect against legal risk.

For employee purposes -personal information gathered during the recruitment process will be retained for the duration of employment and in accordance with the privacy notice for employees and workers. Personal information which is no longer to be retained will be securely and effectively destroyed or permanently erased from our IT systems and we will require third parties to destroy or erase such personal information where applicable,

Data- subject your individual rights

As a data subject you have a number of statutory rights. Subject to certain conditions, and in certain circumstances you have the right to:

- Request access to your information – this is usually known as making a data subject request and it enables you to receive a copy of your personal information we hold about you and to check that we are legally processing it.
- Request rectification of your personal information- this enables you to have any inaccurate or incomplete personal information we hold about you corrected.
- Request the erasure of your personal information- this enables you to ask us to delete or remove your personal information where there is no compelling reason for its continued processing, e.g. it is no longer necessary in relation to the purpose for which it was originally collected.
- Restrict the processing of your personal information- this enables you to ask us to suspend the processing of your personal information, e.g. if you contest its accuracy and so want us to verify its accuracy.
- Object to processing of your personal information- this enables you to ask us to stop processing your personal information where we are relying on the legitimate interests of the business of our legal basis for processing and there is something relating to your particular situation that makes you decide to object to processing on this ground
- Data portability- this gives you the right to request the transfer of your personal information to another party so that you can reuse it across different services for your own purpose.

If you wish to exercise these rights, please address requests to: FOA, Emily Maskell, Data Protection Officer, The London Acorn School, Morden Cottage, Morden Hall Park, London SM4 5JD or email Emily@thelondonacornschoo.co.uk or telephone 020 85449769

We may need to request specific information from you to verify your identity and check your right to access the personal information or to exercise any of your other rights. This is a security measure to ensure that your personal information is not disclosed to any person who has no right to receive it.

In the limited circumstances where you have provided your consent to the processing of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. This will not, however, affect the lawfulness of processing based on your consent for that specific processing based on your consent before its withdrawal. If you wish to withdraw your consent, please contact our Data Processing Officer (as detailed above). Once we have received notification that you have withdrawn your consent, we will no longer process your personal information for the purpose you originally agreed to, unless we have another legal basis for processing.

Please also contact the Data Protection Officer to seek further advice in the following circumstances:

- If you suspect, there has been a personal data breach.
- If you believe personal data are no longer being kept securely or being accessed without proper authorisation.
- If you suspect, there has been any other breach of this policy or any breach of the data protection principles.

Complaints

If you believe that TLAS has not complied with your data protection rights, you have the right to make a complaint to the Information Commissioners Office (ICO) at any time. The ICO is the UK supervisory authority for data protection issues. If you wish to lodge a complaint or seek advice from a supervisory authority please contact The Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF [Tel:+44\(0\) 01625 545 745](tel:+44(0)01625545745) Website: www.ico.org.uk.

Transferring information outside the European Economic Area:

TLAS may transfer your personal information to countries outside the European Economic Area (EEA). However, we would need to seek legal advice on this matter if there is an inadequacy decision by the European Commission in respect to that country. This means that that country to which we transfer your personal information is deemed not to provide an adequate level of protection for your personal information.

Changes to this policy and Review

TLAS will review this policy at regular intervals, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher or nominated representative. TLAS reserve the right to update or amend it at any time and from time to time. Where appropriate, we may notify you of changes by e-mail.

It is intended that this policy is fully compliant with the data protection legislation. However, if any conflict arises between the data protection legislation and this policy, TLAS will comply with the data protection legislation.
This policy may also be made available to the Information Commission on request.