Privacy Notice

Introduction
We at Fostering London take seriously our legal duties and responsibilities in safeguarding your privacy and personal information (data).

This privacy notice aims to inform you of how and why we collect and process the personal information you supply to us; the legal basis upon which we do this; and your rights in respect of data protection.

We advise all our users to read this policy notice and contact us if you have any questions or concerns about our privacy practices.

Data Protection Principles
Fostering London has an obligation to comply with the Data Protection Act (DPA) 1998 and the General Data Protection Regulations (GDPR) 2018 and all legislation and guidance in respect of safeguarding confidentiality. We recognise that the correct and lawful treatment of your data is essential to maintain confidence in our organisation and our business operations and have robust policies and procedures in place.
There are 6 data protection principles that Fostering London must uphold in respect of your data.

- Processed lawfully, fairly and in a transparent manner.
- Processed only for the specified, explicit and legitimate purposes that have been clearly explained to you.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up-to-date
- Kept for no longer than is necessary.
- Processed in a way that ensures appropriate security of the data.

Data Protection Officer
Our Data Protection Officer is Richard Darsa and he is responsible for ensuring that our organisation complies with its legal responsibilities in respect of collecting, processing, storing and sharing personal data. If you have any questions or concerns please do not hesitate to contact him on

Office Address: 34, Shelbourne Road, London N17 9YH
Telephone number: 0208 815 1995 Email: info@fosteringlondon.org.uk

As a fostering agency we collect your personal information in the course of recruiting, approving and supervising foster carers and members of your household and support network. We use the information that you provide to fulfil your request to enquire, apply, become approved and continue your approval as a foster carer with us.
We also collect and process personal information on children and young people who are referred to us and are placed with you.

As an employer we are also required to collect personal information on those who apply to work for us, are interviewed and subsequently are employed or undertake work for us.

Fostering is a public task and we are legally obliged to collect, process, maintain records, store and in certain circumstances share your personal information. We are governed by the Fostering Services (England) Regulations 2011, the National Minimum Standards and are directly accountable to Ofsted.

What personal information we collect?
Fostering London collects personal information at the initial enquiry stage, the application and assessment stage, from approval and throughout your registration as a foster carer with us.

Special Category information
In providing fostering services it is necessary for us to collect, use and store sensitive information about you. This special category information includes personal information such as race, ethnicity, language, religion, sexual orientation, family composition, background as well as the outcomes from our checks. We

are unable to proceed without your knowledge, agreement and signed consent. The exception to this would be where doing it is necessary for our legitimate interests, those of the subject or a third party and your fundamental right do not override those interests for example in matter of safeguarding.
We will need this information to approve you as a foster carer and to continue your registration with us. We recognise and respect the sensitivity of your personal information and ensure that it is handled with the utmost confidentially and stored within our secure computer processing software. All special category data held is in-line with regulations and necessary for the safe provision and management of our fostering service.

Enquiry Stage
You make direct contact with us and register your interest either through our website when you fill in a contact form, via email, social media or call us on the telephone. This interaction will involve you providing us with personal information including your name, address, user names. This personal data will be inputted onto our database. We will not contact you without your initiation.
We are also passed enquiry contact details from Simply Fostering Consultancy. You give your consent to this when submitting the contact form. Their information is stored on a secure social care network, CHARMS. We make contact with you and then you decide whether or not you wish to have any further communication. If you do not wish us to communicate further and let us know we will delete your personal data immediately.

When you visit our website, you will have the opportunity to opt into receiving additional marketing information or newsletters. We will not provide this without your explicit consent and will cease communication with you if you ask us to.

Cookies
We may automatically gather personal data about your browsing actions through the use of cookies and server logs. By default, WordPress generates two types of cookies.
1. Session cookies are set when a user logs in to a WordPress site. These cookies contain a user's authentication details, and the settings for the admin area interface.
2. Login cookies in WordPress expire every 15 days.
The cookies are used for the purpose of understanding visitor behavioural patterns.

Initial Home Visit
If you would like to meet to discuss your enquiry further, we will make a time to visit you. During the course of this visit we will gather additional personal data about you which may include information about your children and adults in the household, childcare experience, employment, criminal convictions, health and motivation to foster. The visiting social worker will explain why we require this information and will not proceed without your consent to do so. You can withdraw your interest at this or any stage.

Fostering Application
If you wish to proceed and we are both in agreement, you will need to make a formal application and complete our application and consent form. The application form requires additional personal information (special category information) including name, date of birth, marital status, nationality, ethnicity, gender, religion, disability, sexual orientation, if you identify as trans, employment, education, health and medical, accommodation, court proceedings, applications to foster or adopt, and details of personal and employment referees. You are asked to sign a declaration, whereby you confirm your understanding and consent to us taking up a series of checks and references. We are unable to proceed with your application without this.
The consent form provides your agreement for Fostering London to make written and verbal checks with the following organisations and individuals including:

- Criminal record check (Enhanced DBS check)
- Local Authority for current address
- Police service/state embassy for another country where lived
- Current employer (including voluntary positions)
- Previous employers (including voluntary positions) where the work involved children or vulnerable adults
- Previous fostering services or adoption agencies
- Schools/colleges currently attended by your children

- Health Visitors where appropriate
- NSPCC
- Personal references as detailed in your application form
- Children including adult children
- Family networks
- Former partners
- Health and safety check

We use your consent to authorise us to complete the necessary checks required for your fostering assessment.

If you or Fostering London decides not to progress your assessment, we will retain the information you and the checks provided for a period of three years from withdrawal. This is in line with the requirements of the Fostering Regulations 2011.

Form F Assessment
If you proceed to a fostering assessment your assessing social worker will explain the assessment process and what this involves. In addition to the above personal data we will also collect personal information on the following:

- Your identity
- Social Media
- Financial information
- Your background history
- Your lifestyle
- Household accommodation including health and safety check
- Motivation to foster
- Support network
- Health and safety
- Capacity/suitability to be a foster carer
- Experience of caring for children and providing structure
- Working with others
- Diversity
- Safer caring.

When the fostering assessment is complete the assessing social worker will present your assessment to our fostering panel who will make a recommendation about your approval. The Agency Decision maker will make a final decision about your registration. All of the information collected during assessment will be held on our secure database. The Fostering Regulations 2011 require us to keep your personal information, including special category information, for a number of years irrespective of whether or not you are approved to foster (see retention periods below).

Post-approval
As an approved foster carer, we have a duty to maintain and update our records and ensure that your checks remain up-to-date including your medical, DBS and health and safety checks.
You will be allocated a supervising social worker who will support, provide regular supervision and supervisory home visits which involve meeting with the foster carers, your children and foster children. All our contacts will be recorded and stored on our database.

We are required to review your approval at least annually. In preparation for the review we will continue to gather personal information about you, members of your household, including children and your support network. A reviewing officer will meet with you and consider all the information gathered and make recommendations in respect of your approval. This is presented to our fostering panel and then to our agency decision maker to make a decision in respect of your continued approval to foster.

Children's Data
We collect and process personal information on children and those under 18 years. Where appropriate we will seek the consent of parents/guardians, those holding parental responsibility and/or corporate parents.

During this process we collect, handle and store personal information with respect and regard for confidentiality and identify the legal basis for doing so.

Data from third parties
During the course of our enquiries, assessment and your approval it will be necessary to collect personal information from third parties. This will include personal information from:

- Financial including bank details
- Updating DBS checks
- Updating our records in relation to the care you provide for children and young people
- Contributions from placing authorities
- Contributions from children and young people
- Your training and learning and development records
- Updating health and medical information
- Complaints or allegations
- Accidents/injuries
- Simply Fostering Consultancy

We will use the personal information provided for the purpose(s) it was collected, unless we reasonably need to use it for another purpose that is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will let you know and explain the legal basis on which we intend to do this.

Where we believe we need to use that data to protect your vital interests or that of a third party you may not be able to provide us with your explicit consent.

Sharing your personal data with third parties
Fostering London is obligated to provide personal data, including special category information with other stakeholders including Ofsted, placing authorities, the police or other law enforcement agencies, statutory agencies and advisory bodies including local safeguarding boards/partners etc. We will give suitable consideration before sharing your special category information with third parties and will only do so where we have a legal obligation and/or with your prior knowledge and consent.
For employees we may be required to provide personal data to HMRC, Ofsted, Local Authorities for contract monitoring purposes and safeguarding, HCPC, the police and other law enforcement agencies and our accountant.

What legal basis do we have for processing your personal data?
In order for Fostering London to be lawful under GDPR we must identify a legal basis for processing your personal data. Fostering London will collect and process your personal information under one of four lawful reasons. This is under consent, contractual necessity, legal obligation and public task. We may process your personal information for more than one lawful ground depending on the purpose we are using it for but will only do so when legally allowed to do so. There are six legal bases:

- Consent
- Contract
- Legitimate interests
- Vital interests
- Public task
- Legal obligation

Consent
We gain your consent prior to the collection of personal information and require your written consent prior to undertaking checks and gathering personal data. We will inform you of the legal basis for purposing and usually inform you if we intend to disclose your information to a third party. Additionally, we require your consent for marketing purposes and enable you to exercise your right to opt in and out by providing relevant tick boxes. You are able to withdraw your consent at any stage of the process.

Contract
We enter into a contract with you when you lodge your interest in becoming a foster carer. It is a contractual requirement for you to provide us with certain personal information in the process of enquiring, applying, being assessed and approved and throughout your approval as a foster carer with us. If you do not provide the relevant information, we are not able to enter into a contract with you and progress any further.

Legal
We will only use your personal data when the law allows and to comply with the legal and regulatory framework that we are governed by as a fostering agency.

Legitimate interests
We will process your personal information where we have a legitimate interest as part of our business management, administrative and operational function.

Public Task
As a registered fostering agency, we collect and process personal information and perform specific tasks, functions and duties that are in the public interest and are set out in law.
We will use your personal information for the purpose it was collected. On occasion we may need to use it for another legitimate purpose if reasonably compatible with the original purpose. If we need to use your personal information for an unrelated purpose where at all possible, we will contact you and explain the legal basis for this unless your fundamental rights are overridden by a third party or permitted by law.

Retention periods
We store your personal information securely and will only do so for as long as is necessary and we are legally obliged to do so. We comply with the retention periods as set out in the Fostering Regulations 2011 and the National Minimum Standards. This will vary according to its type, sensitivity and reason for collection and retention. After which time the data will be destroyed unless required for a legitimate purpose and we are lawfully obliged to do retain. There are three options for destruction of data are removal by overwriting, degaussing or physical destruction. We select the most suitable depending upon the data concerned.

Type of data	Retention period	Legal Basis
Pre-approval		
Enquiry stage/initial visit Identity Contact	6 months after first contact	Consent/legitimate
Fostering Application/ Stage 1 checks/Form F Identity Special category Contact Financial Criminal Medical Social/relationship Education/training Employment	3 years from refusal or withdrawal	Consent/contract/egal

Post-approval As above and Case record Placement records Placing Authority records including safeguarding Accidents/injuries/Ofsted notifications Foster carer reviews	10 years after closure deregistration.	Contract /Legal/public task
Children's records Identity Special category Contact Education Social Medial and health Placement records Placing authority records Accidents/injuries/Ofsted notifications Complaints/allegations/schedule 7 reports	75 years from date of birth of child or 15 years from death if under 18.	Public task/legal
Data analytics and marketing Identity Contact Technical Marketing and communications	For performance of task	Legitimate interest
Meeting internal/external Audit requirements Ofsted data monitoring Placing authority monitoring Monthly internal audits Directors' meetings	For performance of task	Contract/legitimate interest/ public interest
Staff Employment Staff application forms/ Interview records	6 months from date of interview (if not employed)	Time limits on litigation
Staff files Identity/ checks/ contact Supervision notes/ appraisal/grievance/ Disciplinary/Personal development plans	6 years from end of employment	Contract/legal
HMRC Paye/Income tax/pension/ NI/accountant	3 years from end of financial year record relates	Legal

Sharing personal data outside the EEA

Where we share your personal information, we will ensure that the appropriate legal framework is in place. It is not anticipated that we will share your personal data outside of the European Economic Area. However, should this be necessary, we will share your data based on the rules of GDPR, ensuring appropriate levels of data privacy protection and detail the legal basis upon which we do this.

Data Privacy Impact Assessment (DPIA)
A DPIA is an assessment process to help identify, assess and minimise the data protection risks from a project. A DPIA will be carried out when making changes to an existing system or service and is likely to result in a high risk to the privacy of individuals.
The DPIA must

- Describe the nature, scope, context and purpose of the data collection and processing. The purpose is to design more efficient and effective ways of handling personal data and minimising privacy risks.
- Assess the necessity for data use ensuring compliance with the law and regulations.
- Exercising proportionality according to the level of special category information being collected or processed.
- Identity and assess any risk to individuals.
- Take appropriate action and additional measures if required to mitigate the risk.

How do we secure personal data?
Fostering London is committed to ensuring that your personal information is kept secure and we have appropriate security measures to prevent it from accidental loss, unauthorised access, damage or destruction. We use a social care database and Dropbox, a file hosting system to manage and store our data for all aspects in the recruitment, assessment, approval, training, HR and financial management. Our social care database has been developed in the United Kingdom and is hosted on NCSC Cloud security and has ISO Accreditations. The solution is protected by Cisco Firewall Hardware and Software Security Solutions and are protected from Malware by IOMART. Dropbox is hosted in Europe, has ISO Accreditations with premier information and security management with cloud security with multi-layer protection including safe data transfer, encryption and network configuration.

We have suitable electronic and management security systems in place to safeguard your personal data.

We limit access to your personal data on a need to know basis only including employees, agents, contractors and other third parties. Those accessing your data will do so in an authorised manner and subject to conditions set out in our confidentiality policy.

In order to ensure that your personal data is secure we have put in place the following safeguards:

Accessing our server All our data is stored on our secure server which is hosted and managed in the United Kingdom. Our server is password protected and only allows access to those authorised and we restrict access according to the requirements of each post.

Accessing personal data We will only allow authorised staff and third parties to access data who have a legitimate interest and on a need to know basis.

Electronic and paper disposal All paper documents are shredded to ensure their safe disposal. All staff and users are required to routinely dispose of data when it is no longer required to be held for the purpose it was originally created or held or without express permission. All downloaded documents will be deleted and the recycle bin emptied following completion of the task.

Out of use IT equipment All out of use IT equipment will undergo an appropriate data overwrite procedure to ensure information is irretrievably destroyed.

Removable digital media, CDs, DVDs USBs These should not be used without the express permission of the senior managers. If used then they should be stored safely and securely in locked cupboards and only accessed by authorised users. When no longer required they should be deleted and/or destroyed to the extent that the data is irretrievable.

Accessing premises We only allow access to staff and visitors whose identity we have verified to access our premises.

Secure lockable desks We seek to minimise the use of paper records and files but where necessary we ensure that all confidential information is stored in lockable desks and cupboards. Laptops and IT devices should not be left unsupervised when accessing personal information and should be closed down if left unattended. All laptops and IT devices are placed in a lockable cupboard when not in use.

Firewalls and encryption The system is protected by Cisco Firewall Hardware protection and encryption technology.

Updating IOMART have a process in place to ensure the prompt installation of the latest software updates and security patches Cyper essentials, NSCS Cloud Security and ISO Accreditations.

Event logging and monitoring The ICT system have event logging enabled for monitoring and reporting.

Risk assessment and management IOMART undertake regular risk management assessments on the solution and have measures in place to mitigate the risks and bring them to an extremely low level. This ensures business continuity and disaster recovery.

Security Awareness Fostering London ensures security awareness for all staff and users throughout our organisation. This forms part of induction training and on-going training.

Incident response and recovery IOMART has a defined and implemented security incident response and disaster recovery capability, produce and test information security incident management response plans and train the incident management team appropriately.

Notification of data breaches
Fostering London will do all we can to protect and respect your personal data. However, even with our safeguards, it is possible that a security breach may take place. In such an event involving the suspected or accidental loss, destruction or unauthorised access or otherwise of personal data, we have sufficient policies and procedures in place to identify and assess its impact.
Depending upon the outcome of the assessment we will notify the affected parties and where necessary and are legally required to, we will inform the supervisory authorities including the Information Commission Office.

Data breach procedure in the event of a loss
In the event of a data breach we seek to identify as quickly as possible. We isolate the system to prevent spread and disconnect the breached user account. Once contained the threat is eliminated, depending upon the type of attack. Once stopped, an investigation and assessment of the damage to minimise risk of further attack and to check affected systems for any possible left-over malware. The assessment considers the type of data affected, whether this contains high-risk information and if the data was encrypted and can it be restored. We notify authorities, third parties, organisations and individuals affected citing date and nature of the breach and what the recipient can do to protect from further damage. A security audit is conducted to assess the organisation's current security systems and to help with preparation for future recovery plans. The final step is to update the recovery plan including review of new privacy policies and security training for employees.

Appropriate staff data protection training
Staff, Foster Carers and Panel Members undertake GDPR and confidentiality training as part of their induction and this is refreshed within our training and supervisory discussions. All are required to read and sign their understanding of this policy and practice implications. A privacy policy has been created for children/young people.

Monitoring system
Our personal data audit maps the 5 W's; Why, Who, What, When, Where. This is used to monitor compliance and considered at leadership meetings. Monitoring is evidenced, regularly reviewed and communicated to all staff.

Your rights
You have certain rights in relation to the personal data that you provide us with or we collect about you. These rights are legally binding and must be upheld. We will always seek to comply with your requests and carry out our legal duties.

Informed: You have the right to be informed about the collection and use of your personal data in a transparent way.

Access: You have a right to see the personal information that we hold about you, together with how and why we are using this, with whom we may have shared it and for how long we intend to retain it. This is subject to a data access request. Please note that certain conditions apply, particularly in relation to third party information and if we are unable to share any information with you, we will explain why.

Data rectification: You have the right to ask us to correct any information that we hold which is a mistake, inaccurate or incomplete.

Data erasure You have the right to be forgotten and ask us to delete any information we hold about you. Please note that there are certain conditions that apply, particularly in relation to our legal obligations and if we are unable to do so we will explain why.

Ceasing You have the right to request that we stop using your personal information in the following circumstances: it is inaccurate, is used unlawfully, we no longer need to use or have a legitimate reason for doing so.

Please note there may be circumstances where we continue to store or use your personal information for the purpose of legal proceedings or protecting the rights of any other person.

For more information about your rights please see the UK guidance from the Information Commissioners Office on your rights under GDPR.

Complaints
If you are unhappy, have an objection or complaint about any aspect of our data protection, we will try to resolve it swiftly and to your satisfaction. For further details please read our Complaints and Representations procedure.
You will need to put your complaint in writing. We will send you a written acknowledgment within 10 days of receipt. We will ask for any clarifications needed at this stage to proceed with our investigation. Our Data Protection Officer investigate and respond to you within 28 days of receiving the request.

Alternatively, if you are not satisfied and believe we are not complying with the laws and regulations you have a right to make a complaint to:

The Information Commission Office

Telephone number 0303 123 1113

Address: Wycliffe House, Water Ln, Wilmslow SK9 5AF

BP/February 2021