Privacy Notice

March 2022 update

Introduction

- Fostering London takes seriously our legal duties and responsibilities in safeguarding privacy and personal information (data).
- This privacy notice aims to inform people of how and why we collect and process the personal information supplied to us; the legal basis upon which we do this; and rights in respect of data protection.
- We ask all our users to read this privacy notice and contact us if there are any questions or concerns about our privacy practices.
- Fostering London complies 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 personal data is essential to maintain confidence in our organisation and have robust policies and procedures in place.
- There are 6 data protection principles that Fostering London must uphold in respect of data.
- Processed lawfully, fairly and in a transparent manner.
- Processed only for the specified, explicit and legitimate purposes that have been clearly explained.
- 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.
- Our Data Protection Officer is responsible for ensuring that our organisation complies with its legal responsibilities in respect of collecting, processing, storing and sharing personal data. Contact for any questions/concerns:
  Office Address:34, Shelbourne Road, London N17 9YH; Tel. No. 0208 815 1995; Email: info@fosteringlondon.org.uk

What we collect

Foster Carers/Potential Foster Carers

- We collect personal information in the course of recruiting, approving and supervising foster carers and members of their household and support network. We use the information that is provided to fulfil requests to enquire, apply, become approved and continue approval as a foster carer with us.
- Fostering is a public task, and we are legally obliged to collect, process, maintain records, store and in certain circumstances share personal information. We are governed by the Fostering Services (England) Regulations 2011, the National Minimum Standards and are directly accountable to Ofsted.
- In providing fostering services it is necessary for us to collect, use and store sensitive information. This special category information includes personal information such as race, ethnicity, language, religion, sexual orientation, family composition, health, background as well as the outcomes from our checks. We are unable to proceed without 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 the fundamental rights do not override those interests for example in matters of safeguarding.
- We will need this information to approve foster carers and to continue registration with us. We recognise and respect the sensitivity of 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:** When someone makes direct contact with us and registers interest (either through our website when completing a contact form, via email, social media or calling on the telephone), this interaction will involve providing personal information including name, address and user names. This personal data will be inputted onto our database. We will not contact people without initiation.
- We are also passed enquiry contact details from Simply Fostering Consultancy. People give consent to this when submitting the contact form. Their information is stored on a secure social care network, CHARMS. We make contact with the person and then they decide whether or not to have any further communication. If people do not wish us to communicate further and let us know, we will delete personal data immediately.

- When visiting our website, people have the opportunity to opt into receiving additional marketing information or newsletters. We will not provide this without explicit consent and will cease communication if asked 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 enquirers would like to meet to discuss their enquiry further, we set a visit up. During the course of this visit we gather additional personal data which may include information about 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 consent to do so. Enquirers can withdraw interest at this or any stage.
- **Application:** If there is a wish to proceed and we are in agreement, an application needs to be made by completing our application and consent forms electronically. 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. Applicants are asked to sign a declaration, whereby they confirm understanding and consent to us taking up a series of checks and references. We are unable to proceed with applications without this.
- The consent form provides 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 children; Health Visitors where appropriate; NSPCC; Ofsted; Personal references as detailed in the application form; Children including adult children; Family networks; Former partners
- We use the consent form to authorise us to complete the checks required for fostering assessment.
- If the applicant or Fostering London decide not to progress assessment, we will retain the information 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 proceeding to a fostering assessment the 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 the assessment to our fostering panel who will make a recommendation about your approval. The Agency Decision Maker will make a final decision about registration. All of the information collected during assessment will be held on our secure database. The Fostering Regulations 2011 require us to keep personal information, including special category information, for a number of years irrespective of whether or not a person is approved to foster (see retention periods below).
- **Post-approval:** For approved foster carers, we have a duty to maintain and update our records and ensure that checks remain up-to-date, including medical, DBS and health and safety checks.
- Carers are allocated a supervising social worker who will support and provide regular supervisory home visits, which involve meeting with the foster carers, their children and foster children. All our contacts will be recorded and stored on our database.
- We are required to review carer approval at least annually. In preparation for the review we will continue to gather personal information about the foster carer, members of their household, including children and support network. A reviewing officer will meet with carers and consider all the information gathered and make recommendations in respect of approval. This is presented to our fostering panel for the first and at least every third review thereafter for their recommendation. The Agency Decision Maker makes the final decision about continued approval, either directly or following panel if relevant.

Children/Young People

- We collect and process personal information on under 18s living in a fostering household. Where appropriate we will seek the consent of parents/those holding parental responsibility.
- We also collect and process personal information on children and young people who are referred to us and placed in foster homes.

Employees and Contractors

- 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.

Processing data

Legal basis for processing

In order for Fostering London to be lawful under GDPR we must identify a legal basis for processing personal data. We may process personal information for lawful grounds 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:** We gain consent prior to the collection of personal information and require written consent prior to undertaking checks and gathering personal data. We inform people of the legal basis for purposing and usually inform them if we intend to disclose information to a third party. Additionally, we require consent for marketing purposes and enabling people to exercise their right to opt in and out by providing relevant tick boxes. People can withdraw consent at any stage of the process.
- **Contract:** We enter into a contract when a person lodges interest in becoming a foster carer. It is a contractual requirement for them to provide us with certain personal information in the process of enquiring, applying, being assessed and approved, and throughout approval as a foster carer with us. If the relevant information is not provided, we are not able to enter into a contract and progress any further.
- **Legal obligation:** We only use 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 process personal information where we have a legitimate interest as part of our business management, administrative and operational function.
- **Vital interests:** We may need to process personal data to protect their or another person's vital interest, for example matters of public health or public safety.
- **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.

Sharing 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 safeguarding children partnerships. We will give suitable consideration before sharing special category information with third parties and will only do so where we have a legal obligation and/or with a person's 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, SWE, the police and other law enforcement agencies and our accountant.

Sharing personal data outside the EEA

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

Retention of data

- We store 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. After the required retention period, the data will be destroyed. The 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	6 months after first contact	Consent/Legitimate interests
Pre-approval - Application/Stage 1 checks/Form F	3 years from refusal/withdrawal	Consent/Contract/Legal obl.
Post-approval of foster carer	10 years after closure/deregistration	Contract/Legal obl./Public task
Children's Records	75 years from date of birth or 15 years from death if under 18	Public task/Legal obligation
Data Analytics and Marketing	For performance of task	Legitimate interests
Meeting internal/external audit requirements	For performance of task	Contract/Legitimate interests/ Public task
Staff application/interview- not employed	6 months from date of interview	Time limits on litigation
Staff files	6 years from end of employment	Contract/Legal obligation
HMRC and all financial information	6 years	Legal obligation

Security

Securing personal data

- Fostering London is committed to ensuring that 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 personal data.
- We limit access to personal data on a need to know basis. Those accessing data will do so in an authorised manner and subject to conditions set out in our Confidentiality Policy.
- In order to ensure that personal data is secure we have put in place the following safeguards:

- **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 notice has been created for children/young people.
- **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.
- **Lockable storage** - 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 or cupboards. Devices are not left unsupervised when accessing personal information and are closed down if left unattended.
- **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 Cyber essentials, NSCS Cloud Security and ISO Accreditations.
- **Event logging and monitoring** - The IT systems 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 ongoing 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.

Data breaches

- Fostering London do all we can to protect and respect 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 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 Commissioner's Office.
- We will seek to identify any external breach as quickly as possible. We will isolate the system to prevent spread and disconnect the breached user account. Once contained, the threat will be eliminated, depending upon the type of attack. Once stopped, there will be 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 will consider the type of data affected, whether this contains high-risk information and if the data was encrypted and whether it can be restored. We will 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 will be conducted to assess the organisation's current security systems and to help with preparation for future recovery plans. The final step will be to update the recovery plan including review of new privacy policies and security training for employees.

Rights of data subjects

- Everyone has certain rights in relation to the personal data that they provide or that we collect about them. These rights are legally binding and must be upheld. We will always seek to comply with requests and carry out our legal duties.
- **Informed:** The right to be informed about the collection and use of personal data in a transparent way.
- **Access:** The right to see the personal information that we hold, 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. Certain conditions apply, particularly in relation to third party information, and if we are unable to share any information, we will explain why.
- **Data rectification:** The right to ask us to correct any information that we hold which is a mistake, inaccurate or incomplete.
- **Data erasure:** The right to be forgotten and ask us to delete any information we hold. Certain conditions apply, particularly in relation to our legal obligations, and if we are unable to do so we will explain why.
- **Ceasing:** The right to request that we stop using 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 personal information for the purpose of legal proceedings or protecting the rights of any other person.

For more information about rights please see the UK guidance from the Information Commissioner's Office on everyone's rights under GDPR.

Complaints

If a person is unhappy, has an objection or complaint about any aspect of our data protection, we will try to resolve it swiftly and to their satisfaction. Further details are in our Complaints and Representations Policy.
Alternatively, if a person is not satisfied and believes we are not complying with the laws and regulations, they have a right to make a complaint to:
The Information Commissioner's Office; Tel. No.: 0303 123 1113**;** Address: Wycliffe House, Water Ln, Wilmslow, Cheshire SK9 5AF Website – www.ico.org.uk/make-a-complaint Email: casework@ico.org.uk