Data Protection and Information Sharing Policy

Key Elements

This document sets out the responsibilities and expectations for all families of London International Agency in relation to safeguarding and promoting the wellbeing of children and young people at London International Agency

Implementation is monitored by the Director and supported by the Guardianship Organisation with responsibility for Safeguarding

Adopted on:
January 2018

Reviewed on:
January 2018

Agreed by:
London International Agency

Due for Review:
December 2019

The Director of London International Agency (LIA) wishes to make it clear that extremist religious views and partisan political views will not be tolerated.

All families are expected to offer a balanced presentation of views and opinion to children while they are in the care of these families, in attendance at schools and while taking part in extra-curricular activities that are provided or organised by or on behalf of the families or LIA including through the distribution of promotional materials.

Failure to observe the above could lead to procedures including instant removal of the child, cessation of contract without refund and referral to government and education authorities.

London International Agency is committed to protecting the health, safety and welfare of our employees. It is our policy to ensure, as far as is reasonably practicable, that all required tasks and activities are carried out with the minimum of risk to our employees, people in our care and others.

LIA's Data Protection and Information Sharing Policy

Creation Date	Review Date	Version	Director
01/2018	11/2019	2019.01	Krestyna Huggins

DATA PROTECTION

1.0 OBJECTIVE

The Data Protection Act 2018 is legally binding on any organisation or individual who collects or uses personal information about living people.

The Company is fully committed to complying with the requirements of the Data Protection Act of May 2018 which including the **General Data Protection Regulation** (**GDPR**) ("the Act"). The Company will therefore follow procedures that aim to ensure that all employees who have access to any personal data held by the Company are fully aware of and abide by their duties and responsibilities under the Act.

2.0 STATEMENT OF POLICY

In order to operate efficiently, the Company has to collect and use information about people with whom it works. These may include current, past and prospective employees, clients, carers, children, customers, and suppliers. This personal

information must be handled and dealt with properly, however it is collected, recorded or used.
The Company regards the lawful and correct treatment of personal information as very important and fully endorses and adheres to the Principles of Data Protection Act as set out in the Data Protection Act 2018.

3.0 SCOPE OF POLICY

The policy covers all aspects of the company's business relating to personal information and includes all methods of holding and storing information, including:

- Manually stored paper data
- Data stored on computer hard drives and backed up on a secured server
- Computer referenced paper data (e.g. databases)
- Data held in computer applications
- Data held in records archive storage
- Data held on portable storage devices.

4.0 THE PRINCIPLES OF DATA PROTECTION

The Act stipulates that anyone processing personal data must comply with the **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

- Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
- Shall be accurate and where necessary, kept up to date;
- Shall not be kept for longer than is necessary for that purpose or those purposes;
- Shall be processed in accordance with the rights of data subjects under the Act;
- Shall be kept secure i.e. protected by an appropriate degree of security; organisational measures taken against accidental loss or destruction of or damage to personal data.
- Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Act provides conditions for the processing of any personal data and gives descriptions of what constitutes certain types of data.
Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller (the Company); and

- Includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to the individual's:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual orientation;
- Criminal allegations;
- Criminal proceedings or convictions.

In social and health care environments there is also **confidential person identifiable information** which is any data or information relating to:

- Children in the Company's care
- Vulnerable Adults
- Staff working for the Company in any capacity/contract type.

5.0 HANDLING OF PERSONAL/SENSITIVE INFORMATION

The Company will, through appropriate management and the use of strict criteria and controls:

- Collect and process this data in order to fulfil the requirements of the Acts of Parliament and Regulations that govern the operations of the business of the Company;
- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Ensure the quality of information used;
- Ensure personal data is accurate and, where necessary, kept up to date.
- Apply strict checks to determine the length of time information is held;
- Have in place a process by which the length of time data is held meets the requirements of the Regulations in force at the time. See Appendix 1;
- Take appropriate technical and organisational security measures to safeguard personal information. See Appendix 2;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.
- Have a process in place for people to access their data, through subject access requests, see Appendix 3
- Ensure that any information that does not need to be accessed regularly, but which still needs to be retained should be safely archived or put offline.
- Be registered with the Information Commissioner's Office.

6.0 STAFF RESPONSIBILITIES

Every member of staff has a responsibility to protect the data that they come into contact with. Staff will be made aware of their responsibilities under this policy by their line manager through induction, staff briefings and ongoing training. Staff who have access to personal information must ensure that they take good care when disposing of any such documents and must shred these documents wherever possible.
All staff with access to personal information and data must ensure that they deal with it appropriately in accordance with the Company's policies and procedures. It is the responsibility of individual staff members to protect personal data and to report instances of people trying to obtain information by deception or loss of data either accidentally or deliberately.

Note: Any disclosure that can be attributed to an employee's wilful neglect of this procedure will be considered as a breach of procedure and will be dealt with via the Company's disciplinary procedure.

Staff with access to personal information must ensure that they take good care when disposing of any such documents and must shred these documents wherever possible.
Care must also be taken when sending information that contains personal information. All such documents must be stamped Strictly Private and Confidential.

7.0 DATA THAT IS LIKELY TO CAUSE SUBSTANTIAL DAMAGE OR DISTRESS

If an individual believes that the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person, he/she may notify the company in writing to the Director to request the company put a stop to the processing of that information.
Within 21 days of receiving the notice, the company will reply to the individual stating either:

- That it has complied with, or intends to comply with the request; or
- The reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

APPENDIX 1

RETENTION/DISPOSAL OF DATA
1.0 GUARDIANSHIP HOMES

The Company's guardianship homes are required to hold records (paper and/or electronic) safely and securely and retain them for specific periods of time. These records must comply with the following regulations.

- The Children's Act 2004
- Data Protection Act 2018.

The Company stores data in three ways according to its type and how it is to be used operationally.

- Paper records and files
- Google Drive database – regular recording and reporting on all aspects of guardianship activity
- Business Computer Drives – storage on a secure server of documents relating to guardianship activity.

Guidelines are available to staff on how and when to store/retrieve data from these systems.
The Regulations set out how long certain types of records are to be retained, the chart below summarises the current requirements.

APPENDIX 2

Safeguarding of Personal Information

1.0 PAPER DOCUMENTS

All paper documents containing confidential person identifiable information is to be stored in a locked cabinet or drawer with access restricted to staff members who need to process that data.

Particular care must be taken when transporting manual records away from the Company, for example manual records which need to be worked on at home. In this situation, the Company's Data Protection policy will still apply and documents should be kept secure at all times and not exposed to the risk of theft or damage.

Care must also be taken when sending by post information that contains personal information. All such documents must be stamped Strictly Private and Confidential and sent by a recorded delivery service.

2.0 DISPOSAL/REMOVAL OF DATA

Paper documents are to be shredded on site or sent away in secure, traceable bags to be shredded by an approved contractor.

Electronic data will be selected for removal at the appropriate time and deleted by the system administrator.

3.0 DISPOSAL OF COMPUTER HARDWARE

If a piece of computer equipment is to be disposed of, the owner of the equipment must ensure that all personal data on the internal memory (hard drive) is removed before disposal. It will not be sufficient to just 'delete' the unwanted files; they must be permanently removed by overwriting it or taking out the memory storage device in the machine (i.e. Hard Disk).

If any Company location intends to dispose of a piece of computer equipment they should contact the system administrator to arrange for the memory storage device e.g. hard disk to be removed before the machine leaves the premises or to have the machine disposed of by an accredited contractor. All computer equipment disposals must be authorised by the system administrator.

4.0 STORAGE OF CONFIDENTIAL PERSON IDENTIFIABLE INFORMATION ON PORTABLE DEVICES

No data of this type is to be stored on any portable device including laptop computers, mobile phones, tablets, USB or other mass storage devices. The company systems are such that ALL personal data can be stored securely on the secure server or on the secure database. Where it is considered necessary to store this type of data on a portable device, permission must be obtained from a senior manager and the data is to be encrypted. The device is also to be password protected where possible. The senior manager authorising this action is to contact the system administrator to organise data encryption through the approved IT contractor. Any breach of these requirements will be considered a disciplinary issue. As soon as the data is no longer required to be in the device it should be transferred to a server or desktop computer and removed permanently from the memory stick or other external storage device. If on a CD, this should be destroyed.

When it is necessary to transfer or move personal data and it cannot be done by email, it should be stored on an external storage device which is kept in the personal possession of the staff member or stored securely away e.g. in a locked safe place. If it is necessary to store personal data it should be stored on a server, on SharePoint or on a protected desktop computer.

Portable devices are not to be left in an unattended vehicle or on any public transport for any reason.

If it is not possible to email the data and it is necessary to send a memory stick or CD to someone by post it must be sent by the most secure method available to you. At no time must personal data be sent by ordinary post. Personal data must only be sent by a registered, signed for, mail service so that it can be tracked and its safe delivery confirmed by a signature. It should be enclosed in a robust envelope, marked 'Private and Confidential' to the addressee only.

5.0 ELECTRONIC SYSTEM SECURITY

All computers used by the company will be password protected and the system administrator will regularly have all passwords changed. No password is to be displayed on a computer or monitor.

A user leaving their laptop or desktop computer should ensure that they lock their computer (by holding Ctrl + Alt + Del and then choosing 'lock this computer') for the duration they are absent from their desk.

Access to the Google Drive database will be managed by the Director who will organise that permissions at the correct level and passwords are controlled and managed appropriately. When staff leave the company's employment the system administrator will remove all permissions and password access to all company systems.

6.0 DATA SHARING (ENCRYPTION)

The systems used on a day to day basis to email and send data, to and from the servers, is considered safe and secure. Where a request is made to supply encrypted data arrangements need to be made with the IT contractor to facilitate this. There is a cost to encrypt data so it should only be done when absolutely necessary and with the permission of a senior manager who will have to authorise the encryption 'set up' through the system administrator.

7.0 DATA BREACHES

Where an employee knows that there has been a data breach i.e. that confidential person identifiable information has been sent to the wrong location or has been 'lost' they are to report the loss immediately to their manager and the system administrator. The system administrator will take appropriate action and investigate using a checklist based on the HSCIC SIRI (Health & Social Care Information Centre – Serious Incident Requiring Investigation) guidance. Any staff member who knowingly does not report a data loss may be subject to disciplinary action.

APPENDIX 3

RIGHT OF ACCESS TO PERSONAL DATA

Individuals who want to see a copy of the information an organisation holds on them may make a written request in accordance with the Data Protection Act 1998 and pay a fee to see that information.

1.0 PROCEDURE FOR MAKING A SUBJECT ACCESS REQUEST

Requests must be made in writing, to the Director. For people who have a disability under the Equality Act and who are unable to make a request in writing, they should contact the Director for advice and assistance on how to make their subject access request.

The request should include as much detail as possible regarding the information asked for (e.g. where and by whom information is believed to be held, specific details of information required etc) and the individual should provide documented evidence of who they are (e.g. driving licence, passport, birth certificate).

The person making the request is not required to state WHY they wish to access the information: the details we require are merely those that will aid the efficient location and retrieval of information.

There is a £10 fee payable to the Company (permitted under the Data Protection Act 2018) to cover the administration costs of the Subject Access Request process. The Company adopts a general policy of openness in terms of allowing individuals access to their personal information and wherever possible we aim to waive the £10 administration fee. For example, when information can be emailed to the recipient.

Once the Director receives a Subject Access Request, all efforts will be made to fully comply within 40 days. In any event, you will receive all the information that has been located and can be released within 40 days and an explanation for any information that cannot be provided at that time. The 40 days will start from the date that we receive full payment and all of the required information to locate the data requested.

In accordance with the Data Protection Act 2018, the Company does not usually release information held about individuals without their consent. Therefore if information held about you also contains information related to a third party, the Company will make every effort to anonymise the information. If this is not possible, and the Company has been unable to secure the relevant consent, the Company may decide not to release the information.

In relation to references received through the recruitment process, LIA is not the author and therefore does not own this information. If an applicant wishes to obtain copies of their references, the applicant needs to contact the author directly and ask them to release this information to them.

Reasonable intervals must elapse between the first subject access request made and any subsequent requests made by the same person. Any member of staff receiving a request under the Data Protection Act should seek advice from the Director.

4.0 FURTHER INFORMATION

If you require further information contact Krestyna Huggins, the Director London International Agency.

Adoption Date	Review Date	Director
01/2018	**11/2019**	**Krestyna Huggins**