Data Protection Policy

Overview

AFA needs to collect and use certain types of data in order to carry out its work. This personal information must be collected and dealt with appropriately and AFA is committed to protecting the rights and privacy of individuals in this regard.

Everyone has rights as to how their personal information is handled and used. During the course of its activities, AFA will collect, store and process personal information about applicants, Foster Parents, support carers, employees and the children and young people it has responsibility for. AFA recognises the need to treat all information in an appropriate manner, in line with current legislation.

All information, which may be held on computers, laptops and mobile devices, or in a paper file, and which includes email, minutes of meetings, and photographs, is subject to legal safeguards as specified in the General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant regulations that impose restrictions on how AFA uses information.

AFA will remain the data controller for the information held, with the exception of data held in relation to children looked after. In this regard, AFA will be a joint controller with the responsible Local Authority in respect of this data for the duration of the time the child lives with its Foster Parents.

Employees, Contractors (including Panel Members & Volunteers) and Foster Parents who have access to personal information must read and comply with this policy.

Purpose

The purpose of this policy is to set out AFA's commitment for protecting personal data. AFA regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom it deals.

The General Data Protection Regulation (UK GDPR)

The UK GDPR has two core purposes:

- To regulate the use by those (known as data controllers) who obtain, hold and process personal data on living individuals
- To provide certain rights (for example, accessing personal information) to those Data Subjects for whom whose data is held

Anyone processing personal data must comply with the Six Data Protection Principles contained within the UK GDPR. These state that personal data must be:

- Principle 1: Fairly and lawfully processed
- Principle 2: Purpose: collected for specified, explicit and legitimate reasons
- Principle 3: Adequacy: relevant and limited to what is necessary

- Principle 4: Accuracy: personal data shall be accurate and where necessary kept up to date
- Principle 5: Retention: personal data processed for any purpose/s shall not be kept for longer than is necessary for that purpose/s
- Principle 6: Rights: personal data shall be processed in accordance with the rights of the Data Subject

AFA are also responsible for, and must be able to demonstrate compliance with, accountability to the above principles, sometimes known as the 7th Principle.

Further information relating to the Data Protection Principles can be found on the Information Commissioner's Office website, **www.ico.org.uk**

Useful Definitions within the UK GDPR

The following is a list of definitions as to technical terms contained within this policy:

Data Controller – The person or organisation who (either alone or with others) decides what personal information will be held and how it will be held or used.

Joint Data Controller – If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers.

Data Processor - The UK GDPR defines a processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person appointed by the organisation who is independently responsible for ensuring that it follows its Data Protection Policy and complies with the Data Protection Act 2018 and the UK GDPR.

Data Subject/Service User – The individual whose personal information is being held or processed.

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about them:

Sensitive Data (Special Categories of Personal Information) – this includes personal data:

- revealing racial or ethnic origin
- revealing political opinions
- revealing religious or philosophical beliefs
- revealing trade union membership
- regards genetics
- regards biometrics (where used for identification purposes)
- concerning health
- concerning a person's sex life
- concerning a person's sexual orientation

Notification – Notifying the Information Commissioner's Office (ICO) about the data processing activities of the organisation.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018 and the UK GDPR.

Processing – Means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about data subjects that enables them to be identified, e.g., names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as self-employed contractors.

Personal Data

"Data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose. This includes computer-generated material.

"Personal data" means data consisting of information relating to a data subject who can be identified from that information (or from that and other information in the possession of a data user), including any expression of opinion about them. In practice, this means any data recorded on AFA's computer systems relating to a living person. Personal Data could also include handwritten notes and is not limited to data kept electronically.

The processing of personal data must comply to the Six Data Protection Principles contained within the UK GDPR as detailed on page 2.

Appropriate security measures must be taken against unauthorised access to, alteration, disclosure, destruction, or accidental loss/destruction of personal data.

Data Breaches

A data breach is where personal information is accidentally or intentionally divulged to third party that does not have a lawful right to receive the information. Data breaches must be reported to the Registered Manager immediately it is discovered.

Data Breaches include, but are not limited to:

- Loss or theft of a system or device that contains personal data
- Loss or theft of paperwork that contains personal information
- Sending an email to the wrong recipient
- Failing to use BCC on group emails that contain personal information
- A successful Cyber Attack, such as a Ransomware attack or misuse of system access.

Data breaches are considered infringements of the rights of data subjects, which is why they must be reported immediately upon discovery.

Data Sharing

From time to time, it will be necessary to share personal information for a lawful purpose such as where a LADO or police investigation is initiated. In any event, all requests for data sharing must be reported to the Registered Manager to ensure the request is appropriate, lawful and follows data sharing procedures including cyber security controls.

Rights of the Individual

A data subject is entitled to be informed whether personal data is held, of which they are the subject, to access any such data and when appropriate, to have such data corrected or erased. Under the UK GDPR, they have the right:

1. to be informed
2. to access
3. to rectification
4. to erasure
5. to restriction of processing
6. to data portability
7. to object
8. in relation to automated decision making and profiling

For further details on the rights of individuals, please visit **www.ico.org.uk**.

There is other legislation, such as the Fostering Regulations 2011, that must be considered when complying with the above rights. Data subjects will be informed of these regulations should they apply to a request made in relation to the above rights.

Right of Access to Records

The provisions for access to personal information or records held by AFA are contained within UK GDPR. Under this legislation, data subjects have a right of access to that information, unless one of the exceptions set out below applies:

- Where practice would otherwise be prejudiced because access to the information would be likely to result in serious harm to the person requesting the information or some other person
- Where a personal or professional reference has been provided in confidence
- Where the person is incapable of managing his or her affairs (for example where the person is a child) and the information was given in the expectation that it would not be disclosed, or is information which the subject of the information expressly indicated should not be disclosed

Access can also be refused if:

- To disclose the information would involve disclosure of information about someone else without that person's consent, and disclosure cannot be justified without that person's consent
- Where disclosure may prevent the detection or investigation of a crime
- An identical or similar request has been received from the same person and has already been complied with, unless a reasonable interval has elapsed

These exceptions do not permit the total withholding of information, but only those sections of the material covered by the exceptions. The remainder of the case records should be made available to the data subject.

The exceptions do not apply where disclosure is required by a Court Order or is necessary for the purpose of, or in connection with, any legal proceedings. However, a Court may prevent disclosure of information where a person shows that he or she would be caused serious harm to his/her physical or mental health by the disclosure.

AFA staff are encouraged, where appropriate, to openly share information and recordings, including providing copies of key documents. If a data subject asks to see a specific document or wants to have information about a particular aspect of the case, the Fostering Social Worker should discuss this with them to see whether the request can be dealt with informally by showing them the relevant part of the recording or providing copies of relevant documents where appropriate and in line with relevant data sharing processes.

The right of access, commonly referred to as subject access, gives data subjects the right to obtain a copy of their personal data as well as other supplementary information. It helps them to understand how and why AFA are using their data, and check AFA are doing so lawfully.

Data Subjects can request the following from AFA:

- confirmation that AFA are processing their personal data
- a copy of their personal data
- other supplementary information

A data subject is only entitled to their own personal data, and not information relating to other people (unless the information is also about them or they are acting on behalf of someone).

How to make a Subject Access Request

A data subject can make a Subject Access Request either verbally or in writing.

Staff in receipt of a subject access request must notify the Registered Manager immediately.

AFA must comply with a request without undue delay and, at the latest within one month of receipt of the request or (if later) within one month of receipt of any information requested to confirm the requester's identity.

AFA may contact the Data Subject to discuss the request as this may help identify the information they require and enable the information to be sent to them sooner. It may also be necessary to seek identification of the requestor if it is unclear that the requestor is the data subject.

If it is not possible to meet the timescales because the request is complex, an extension to the request of up to 2 months to ensure all of the relevant data is provided. If this is required, a written explanation will be provided.

AFA is unable to provide copies of data or documents from third parties. Data Subjects would need to obtain this from the original source. Some exemptions may apply in relation to providing copies of social work data and documents including personal references.

Data Retention

Data and records must not be kept for longer than is necessary. This principle links to UK GDPR, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose".

As an organisation, AFA has a responsibility to protect the integrity and confidentiality of personal data it holds.

Individual employees and Foster Parents also have that obligation with regards to unauthorised disclosure of data, whether it is oral, printed, hand-written or computer based.

This policy has been written to provide the necessary information to AFA employees, Foster

Parents, support carers and Applicants and details their duties under UK GDPR and Record Retention procedures. This policy has also been written to set out the standards expected by AFA employees and Foster Parents in relation to processing of personal data and safeguarding individual's rights.

Please see the AFA Record Retention Schedule, regulatory requirements i.e., OFSTED, Fostering Regulations 2011, National Minimum Standards and framework for keeping up to date with changes in legislation.

Data Storage

All data and records are stored as securely as possible in order to avoid potential misuse or loss. The degree of security required for data storage reflects the sensitivity and confidential nature of any material recorded. All data and records are stored in the most appropriate location having regard to the period of retention required and the frequency with which access will be made to the record. When such data has been earmarked for destruction, appropriate measures are taken to ensure that the data cannot be reconstructed and processed by third parties.

Children's Data

All paperwork for children who are looked after is returned to the responsible Local Authority. AFA holds electronic files in its archive for 7 years after a child turns 18, unless they, as Data Subject, request that the data is deleted from AFA's computer system.

Safeguarding

AFA is a social work agency, and as such has a core responsibility to safeguard children and vulnerable adults. This will sometimes involve the sharing of information with other people, professionals and/or organisations in an unredacted format, and may (on a case-by-case basis) be undertaken under any or all of the lawful bases of 'legal obligation' , performance of a contract' and 'legitimate interests' (Article 6 of the UK GDPR) as identified by the ICO at: **Linked to ICO lawful basis for processing**

In such cases AFA will complete the following checklist of compliance to ensure it has:

- reviewed the purposes of its processing activities and selected the most appropriate lawful basis (or bases) for each activity
- checked that the processing is necessary for the relevant purpose and is satisfied that there is no other reasonable and less intrusive way to achieve that purpose
- documented the decision on which lawful basis (or bases) applies to help it demonstrate compliance
- included information about both the purposes of the processing and the lawful basis for the processing in its privacy notice
- confirmed, where legitimate interest is deemed the lawful basis for processing, the part Legitimate Interest test will be applied, and the result recorded

Further information

Your full rights under the Data Protection Act and UK GDPR can be found at the Information Commissioner's website: **Your data matters | ICO**

If you have a complaint about the way AFA handle or manage your personal information, please contact:

AFA Data Protection Officer
Guardian Saints CiC
Eagle House
Cranleigh Close
South Croydon
CR2 9LH
0208 300 3878
gsdpo@guardiansaints.com

Connected Policies or Guidance

Name of Policy / Guidance	Relevant for
Foster Parent's Handbook	Foster Parents & Fostering Social Workers
Fostering Social Workers Guidance	Fostering Social Workers and Managers
Recording and Confidentiality Policy	All staff and Foster Parents
Whistleblowing Policy	All staff and Foster Parents
Complaints and Compliments Policy	All staff and Foster Parents
Staff Handbook	All staff
Staff data protection processes	All staff
Foster Parent data protection processes	Foster Parents & Fostering Social Workers

Updated March 2024 Version 2.2