Data Protection Policy

Data Protection Overview

Everyone has rights as to how their personal information is handled and used. During the course of our activities, AFA will collect, store and process personal information about our carers, employees and the children in placement. We recognise the need to treat all information in an appropriate manner, in line with current legislation.

Any information, which may be held on paper, on a computer or other media, is subject to legal safeguards as specified in the General Data Protection Regulation (GDPR) 2018, the Data Protection Act 1998 and other relevant regulations imposes restrictions on how we use information.

Anyone processing personal data must comply with the Six Data Protection Principles. 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 shall not be kept for longer than is necessary for that purpose or purposes.
- Principle 6 Right, personal data shall be processed in accordance with the rights of the data subject.

Access to Records

Rights of access

The provisions for access to personal information or records held by the agency are contained in GDPR 2018. Under this legislation, those for whom personal information is held (in any form) have a right of access to that information, unless one of the exceptions set out below applies.

Access to a Foster Carer's assessment report can, with their permission, be made available to another fostering service if they apply to a that service to become carers.

Exceptions to the right to access are:

- 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 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; or
- 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 service user.

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

Offering an informal approach
Staff should be encouraged to openly share information and recordings, including providing copies of key documents. If a person in receipt of services asks to see a specific document, or wants to have information about a particular aspect of the case, the 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

Handling formal requests for access
Any person making a formal request for access to their records should be asked to put the request in writing. The receipt of the written request should be recorded by staff, who must verify the identification of the person making the request. If he or she is not known personally to those working at the agency, staff must ask for photographic evidence, either a passport or driving licence.

Prior to access being given, all case records held on the person should be located and collected, and the approval of the Area Manager should be sought. If approval is not given, this must be communicated to the person seeking access, giving an explanation.

Staff should carefully check the case records to ensure they are complete and maintained, and to ascertain whether any of the material comes within the exceptions to the rights of access (see Exceptions).

There should be no disclosure of the identity of third parties or other sources of information, which fall within the second exception (see Exceptions).

Any other information supplied by third parties should not usually be disclosed without the third party's consent. When it is not possible to obtain consent, discretion may be used to release information if there is no possibility of serious harm.

An appointment should be made at the earliest opportunity to share the case record with the person making the request, and he or she should be asked to bring appropriate proof of identity.

Staff should be available to explain the contents of the records, to answer questions and to help the person understand the information recorded.

Where the person making the request has specific needs in relation to language or disability, arrangements must be made to present the information in a suitable manner and provide approved interpreters as needed.

Interpretative and supportive counselling may be advisable in certain cases, using a number of interviews to disclose the information, if the person concerned is willing to proceed in this manner.

A request for copies of information disclosed must be met.

Timescales
Access must be given to disclosable information within 40 days of receiving a request. This is the maximum time period allowed. The timescale can only be extended with the agreement of the person requesting access. Where he or she refuses to agree an extension, access should be given to all information open to disclosure at that point.

Applications by children
Requests from children should be treated in the same way as requests from adults. A judgement should be made by the staff, in conjunction with the child's Social Worker, as to whether the child understands the nature of the request. Where appropriate, a parent should be asked to provide written confirmation that the child understands the nature of the application.

Children with disabilities have the same rights as others to have access to information held on them. No assumption should be made about their level of understanding. This should be assessed on an individual basis, as with all children.

A child of sufficient understanding should be allowed regular access to information held about him or her, consistent with his or her best interests. He or she should read or be told what has been recorded unless it falls within one of the exceptions set out above.

A child should be encouraged to record his or her own observations on the case record including any disagreement about an entry in the file.

Applications by parents
If any member of staff considers that the child does not understand the nature of the request, the parent may make a request on the child's behalf. However, the request must be in the interests of the child, rather than the interests of the parent.

If a parent seeks to have access to his or her child's records, the worker dealing with the request must assess whether the child might be able to request access to the records for him or herself. If this is the case, the worker should check that it is the child's choice for the parent to see the records on his or her behalf. If it is, the child will be asked to confirm this in writing and access to files for the parent can then be agreed.

Whether or not a child is capable of understanding the request or has consented to the parent making the request, it is important that a parent should only be given access to the

information about the child if the worker, in consultation with his or her manager, is satisfied that the request is made in the interest of the child and not the parents.

Applications by agents
A request for access to records may be made through an agent (for example, a solicitor). It is the agent's responsibility to produce satisfactory evidence that he or she has authority to have access to the records. This must always include proof of their identity.

The Registered Manager will decide whether the representative will be allowed access, having sought legal advice when necessary.

Applications on behalf of deceased persons
Where a request is received for access to the records of someone who has died, the person making the application should be asked to explain in writing their relationship to the deceased person, what information is needed and why. A staff member should make a decision in consultation with his or her manager and advise the applicant in writing of the decision giving reasons.

Corrections or erasure of records
If a person considers that any part of the information held on his or her records is inaccurate, he or she has a right to apply in writing for it to be corrected or erased. If the objection is justified, there is a duty to correct or erase the identified information.

Refusal of access
A staff member who considers there are reasons to refuse a request for access to all or any part of the records, should discuss this with his or her manager and obtain legal advice.

The Registered Manager should be asked to make a final decision on refusal of access, having sought legal advice if required. If refused, the date of the request and reason for refusal must be recorded in the file.

The decision and the reasons for it should be confirmed in writing to the person requesting access, or in a format appropriate to the needs of the person concerned.

Appeals process
The person concerned has the right to apply to the Court for an order to disclose, correct or erase information held. They also have a right of appeal to the Data Protection Commissioner.

Data retention

As an organization, AFA has a responsibility to protect the integrity and confidentiality of personal data held by us with regard to our clients and employees.

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

This policy has been written to provide the necessary information to AFA employees and carers and details their duties under GDPR 2018 and Record Retention procedures. This policy has also been written to set out the standards expected by AFA employees and carers in relation to processing of personal data and safeguarding individual's rights.

The General Data Protection Regulations(GDPR)
has two core purposes:

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

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 living individual 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 the individual. In practice, this means any data recorded on our computers relating to a living person.

Personal data must be:

- Fairly and lawfully processed
- Collected for specified, explicit and legitimate purposes.
- Relevant and limited to what is necessary
- Personal data shall be accurate and where necessary kept up to date
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or purposes.
- Personal data shall be processed in accordance with the rights of the data subject.

An individual is entitled:

- To be informed whether personal data is held, of which they are the subject;
- To access any such data;
- When appropriate, to have such data corrected or erased.

To comply with the two core principles of GDPR, records containing personal data must be:

- Collected and processed fairly and lawfully
- Stored appropriately;
- Only collected for legitimate purpose.
- Retained for only as long as necessary;
- Disposed of appropriately.
- Processed in accordance with the rights of the data subject.

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

Client data

This section specifically refers to data held about clients and includes the recording, processing and security of personal and sensitive information relating to them and people who work for them. Whilst it is the organisations ultimate responsibility to ensure that personal data held concerning a client is up to date, accurate and taken for lawful purposes, it is the individual employee's duty to ensure that the information is correctly taken from the client and accurately recorded.

It is the organizations' responsibility to ensure that the records and systems are backed up

on a regular basis and to ensure there is no loss or destruction of personal data. If you as an employee are aware of any errors, or have any concerns regarding personal data, this should be reported immediately to AFA's Data Protection Officer (DPO) on 01603 559255

Appropriate action must be taken against:

- Unauthorised access to or alteration, disclosure, or destruction of personal data;
- Accidental loss or destruction of personal data;
- Disclosing personal data or policy details to the general public;
    - ask questions so that you can be reasonably assured that the caller is genuine;
    - establish what information is required - ask yourself;
    - whether the caller is entitled to the information;
    - whether this is a normal business enquiry;
    - whether the caller could have access to the data anyway;
    - be cautious if the caller is not the data subject;
- Discussing/disclosing sensitive information, for example;
    - medical/disability details;
    - employment history;
    - convictions;
    - high value personal belongings;
    - sensitive information – this includes anything identifiable.

Data relating to a client must not be disclosed to third parties unless the client has given express written consent. You must never leave client records unattended or in such circumstances where third parties may gain access to them.

You should adopt a secure filing system and return client records to the filing system when not in use. You must forward all third party requests for details of personal data held by us immediately to AFA's DPO who will deal with the request or will authorise you to do so.

Failure to comply with the above could be treated as misconduct. It is also a criminal offence to hold, use or disclose personal data which needs to be, but is not registered, or to use it for a purpose other than that registered. This offence applies both to the organisation and to the employee concerned.

Guidelines for Data Protection

The guidelines for the data protection, in summary
are:

- Personal data shall be processed fairly and lawfully;
- Personal data 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;
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data.

All data and records will be stored as securely as possible in order to avoid potential misuse or loss. The degree of security required for file storage will reflect the sensitivity

and confidential nature of any material recorded. All data and records will be stored in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

Personal data will not be held for longer than necessary and when such data has been earmarked for destruction, appropriate measures will be taken to ensure that the data cannot be reconstructed and processed by third parties. Any data file or record which contains personal data of any form can be considered as confidential in nature.

Retention

Data and records should not be kept for longer than is necessary. This principle links to statutory form GDPR 2018, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose".

Please see AFA record retention schedule at the end of this Policy, regulatory requirements i.e. OFSTED and framework for keeping up to date with changes in legislation.

Managing your personal emails (Carers)

You have a responsibility to manage this information securely. If you have to send an email to a placement manager, or other professional use initials not names. Once you have recorded sending this on charms delete it from your emails.

Keep things safe, don't write down your email password, keep it longer than 10 characters and change it regularly, don't use the same passwords for multiple accounts.

Returning children paper work at the end of placement

When a placement has ended you will undoubtedly have paperwork relating to the young person that has been sent to you by the local authority, school etc, this needs to be returned to the AFA office.

Please arrange a time to drop this off to ensure there is a staff member available to take receipt.

This needs to be completed within 2 weeks of a placement end and until it is returned must remain in a securely locked cabinet.

Destruction and disposal

To ensure compliance with GDPR 2018, all information, in any format, destroyed from any AFA location must not expose the confidentiality of our employees, clients and customers.

All office paperwork for destruction should be placed in confidential waste bins/ bags if the content is in any way sensitive.

Other paper can be disposed of in the bins provided in offices as long as it contains no sensitive or identifiable information – if in any doubt then it must be shredded.

The procedure for the destruction of Confidential or Sensitive Waste on electronic media such as tape, disk, cassette/cartridge, hard drives, CD-ROM, DVD and ZIP drive is as follows:

Once permission for destruction is agreed by a Senior Manager or Director, it should be

delivered to the office to be taken to EasyPC for destruction. Destruction of back-up copies of such data will also be dealt with in the same manner.

References:
www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/how_does_the_data_protection_act_apply_to_professional_opinions.pdf
http://online.businesslink.gov.uk/bdotg/action/searchBasicMode?resultPage=1&expression=record+retention+ www.acas.org.uk

Connected Policies or guidance

Name of policy / Guidance	Relevant for
Foster Carer's Handbook	Foster Carers and Placement Managers
Whistleblowing Policy	All staff and Foster Carers
Complaints and Compliments Policy	All staff and Foster Carers
Staff Handbook	All staff

AFA record retention schedule

DOCUMENT	***RETENTION PERIOD***	***EXTRA INFORMATION***	***SOURCE***
Sickness, Sick Pay,	3 years	The Statutory Sick Pay (General) Regulations 1982 (SI 1982.894 as amended www.businesslink.gov.uk	
Maternity Leave/pay	3 years after the relevant tax period.	Statutory	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Parental Leave	5 years from birth/adoption of the child or 18 years if the child receives disability allowance	Not statutory.	The maternity and paternity leave etc. paternity and adoption (amendment) 2008 Ref. 1966 www.businesslink.gov.uk
Wages/Salary	6 years recommended after the relevant Tax year 3 years minimum	Taxes Management Act 1970 www.businesslink.gov.uk	
Applications Forms and Interview notes for unsuccessful candidates	6 months to 1 year 1 year recommended	Not statutory, in case of any discrimination challenge.	www.acas.org.uk

DOCUMENT	***RETENTION PERIOD***	***EXTRA INFORMATION***	***SOURCE***
CRB disclosures (Now DBS)	No longer than necessary (6 months) Info held at http://www.civilandcorporate.co.uk/ only outcome and check number are stored.	Contact with Regulating Authority, may wish to check before destroyed	Code of Practice CRB April 2009
Personnel Files	6 years after employment ceases	Not statutory	www.businesslink.gov.uk
Training Records	6 years after employment ceases	Not statutory	www.businesslink.gov.uk
Medical Certificates	4 years recommended	Not statutory	www.businesslink.gov.uk
Disciplinary	6 years after employment	Certain disciplinary records have lapsed time.	www.acas.org.uk
Redundancy	6 years from the date of redundancy	Not statutory	
Recruitment and eligibility to work in the UK	Throughout the period of working and at least 3 years after employment finishes.	Copies of all relevant documents should be retained.	www.businesslink.gov.uk
Duty Rosters	4 years after the year to which they relate	Essential Standards of Quality & Safety (March 2012)	

DOCUMENT	***RETENTION PERIOD***	***EXTRA INFORMATION***	***SOURCE***
Accounting documents for a public limited company and those Ltd by Guarantee	6 years	To cover the time limit for bringing any civil legal action against you, including national minimum wage claims and contractual claims	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Accounting documents for a Private limited company	Minimum 3yrs recommend 6 years	To cover the time limit for bringing any civil legal action, including national minimum wage claims and contractual claims	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Tax Records	6 years minimum	HMRC can charge a penalty if company tax records not kept.	The Income Tax (Employments) Regulations 1993 (SI1993/744) as amended for example by The Income Tax (Employments) (Amendment No 6) Regulations 1996 (SI1996/2631)
Children's Files	"For at least 75 years from the date of birth of the child to whom it relates or the last date of entry. **The Local Authority is responsible for this** – any AFA paper files are returned at the end of placement and electronic file archived with Charms	CQC Essential standards of Quality and Safety- recommends 80 yrs. page 173	The Children's Homes Regulations 2001 Regulation 28(3) Data Protection Act 1998 GDPR 2018

DOCUMENT	***RETENTION PERIOD***	***EXTRA INFORMATION***	***SOURCE***
Foster Carer Files	A record must be kept in relation to each Foster Carer, covering the carer's assessment and approval, children placed, and other matters as set out in regulation 30. This includes Foster Carers who have temporary approval under the 2010 Regulations. The records must be kept for at least 10 years after the Foster Carer's approval ends. There is also a requirement to keep records relating to people who do not go on to be approved as Foster Carers, and to retain these records for 3 years (regulation 32). The fostering service must keep a register of Foster Carers, covering the information set out in regulation 31. This information about Foster Carers should be retained for at least 10 years after their approval has ended. The Service must also keep a register of children placed with Foster Carers and include the information set out in Schedule 2 of the Regulations. This should be kept for 15 years after the date of the last entry (regulation 22). They must also keep a register of Foster Carers, containing the information set out in regulation 31. All records of the service must be kept under conditions of confidential and secure storage so as to prevent their loss or destruction (standards 26 and 27). Premises must be suitable to enable secure storage of records, both paper and electronic.		Fostering Regulations 2011 GDPR 2018

DOCUMENT	***RETENTION PERIOD***	***EXTRA INFORMATION***	***SOURCE***
Contract	6 years	Public service contract regulations 1993 Public supply contract regulations 1995	www.nationalarchives.gov.uk
Contracts under seal	12 years	Public service contract regulations 1993 Public supply contract regulations 1995	www.nationalarchives.gov.uk

DOCUMENT	***RETENTION PERIOD***	***EXTRA INFORMATION***	***SOURCE***
Employers liability	The requirements to retain compulsory employer's liability certificates for 40 years ceased on 1 October 2008, however it is advised to continue to keep this in case of claims.	Tracing Code of Practice includes a commitment from insurers to keep employers' liability records for 60 years.	http://www.dwp.gov.uk /docs/codedocument.p df http://www.dwp.gov.uk /docs/elci-consultation-document.pdf
Hazards substances (Asbestos)	40 years 30 years from the date the substance was received into the work place	Occupational safety and health act (OSHA)	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (Sls 1999/437 and 2002/2677
Industrial Accidents	12 years	Personal liability claims can only be made up to 12 years after the event.	
Accident Books/Reports	3 years	Please note from the 6th April 2012 trigger points for notification will be increased from 3-7 days see www.hse.gov.uk/rid dor/reporting-change.hmt for details	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (Sl 1995/3163) as amended.
Incidents, events or occurrences that require notification to the Care Quality Commission	3 years	Essential Standards of Quality & Safety (March 2010)	
Maintenance of Premises	3 years	Essential Standards of Quality & Safety (March 2010)	
Maintenance of Equipment	3 years	Essential Standards of Quality & Safety (March 2010)	

DOCUMENT	***RETENTION PERIOD***	***EXTRA INFORMATION***	***SOURCE***
Electrical Testing	3 years	Essential Standards of Quality & Safety (March 2010)	
Fire Safety	3 years	Essential Standards of Quality & Safety (March 2010)	
Water Safety	3 years	Essential Standards of Quality & Safety (March 2010)	
Medical Gas Safety, Storage and Transport	3 years	Essential Standards of Quality & Safety (March 2010)	
Purchasing of Medical devices and medical equipment	11 years	Essential Standards of Quality & Safety (March 2010)	

Updated May 2018