General Data Protection Regulation (GDPR) which apply from 25 May 2018. Foster Care Link Policy

Introduction

Foster Care Link as an organisation has responsibility to protect the integrity and confidentiality of all personal data held with regard to clients and employees and any other users of the service.

Unauthorised disclosure of data whether it is oral, printed, hand-written, IT based, electronic files, photographs, external memory sticks, hard drives, CD ROM's, Video, cloud storage, web/media must be avoided.

The named person responsible for Data Management is Ayub Patel, Office Manager;
admin@fostercarelink.com
0208 880 5387.

Additional notes

Any organisation that processes personal information is required to register with ICO Information Commissioners Office and have a named person responsible for Data Management, for guidance please see https://ico.org.uk/for-organisations/register/
An overview of the General data protection regulations is accessible form this link
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Foster Care Link is registered with the ICO, a named person has been established and deputising arrangements in their absence have been identified.

Purpose

This policy has been written to provide the necessary information to Foster Care Link managers, employees and associates detailing their duties under the Data Protection Act 1998 and Record Retention procedures and the new General Data Protection Regulation (GDPR) which apply from 25 May 2018. This policy has also been written to set out the standards expected by MOU employees in relation to Record Retention & Disposal of personal/sensitive data and safeguarding individual's rights.

Scope

This policy covers all records held by Foster Care Link irrespective of the media on which they are created or held, including oral, printed, hand-written, IT based, electronic files, photographs, external memory sticks, hard drives, CD ROM's, Video, cloud storage, web/media.

Minimum Retention Periods

Guidance notes
General Data Protection Regulation (GDPR) requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose".
Regulatory organisations are becoming less prescriptive regarding time scales that records should be kept.

However, organisations such as Foster Care Link are mindful that accurate well organised historical records/documentation that can be accessed are an effective way of

addressing any disputes or investigations. Changes within the employment and pension legislation make the need to retain some aspects of employee information for much longer; including past retirement as advised by.gov.uk

The approved record retention schedule held by Foster Care Link can be used as a guide and adapted as appropriate for organisation.

The recommended times are derived from:

- *The business needs*
- *Legislation*
- *CQC/OFSTED or other regulators such as the HSE*

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 file storage will reflect the sensitivity and confidential nature of any material recorded.

All data and records are 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 will be considered as confidential in nature.

Personal Data what do we mean and how do we keep it safe.

“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 and 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 obtained and processed fairly and lawfully*
- *be held only for the purposes for which it is specifically required*
- *be adequate, relevant and not excessive in relation to those purposes and only be disclosed to appropriate people*
- *be accurate and, where necessary, kept up to date*
- *not be kept for longer than is necessary*
- *be processed in line with the data subjects’ rights*
- *be secure*
- *not be transferred to other countries without adequate protection*

Foster Care Link holds I personal data concerning foster carers registered with them, and their directly employed staff.

Some records are electronic, and these are kept in a specific secure mapped drive with only the two executives having access to this part of the secure drive.

The server is encrypted and backed up at least weekly.

Client Data

This section specifically refers to data held about foster carers, children and any other clients and includes the recording, processing and security of personal and sensitive information relating to them and people who work for them.

It is Foster Care Link's responsibility to ensure that all personal data held is up to date, accurate and taken for lawful purposes. The referring local authority and the service user will give permission to release information to appropriate partner agencies as part of their application for services. The service user has full access to their data and is kept informed.

Additional notes
Foster Care Link through this policy is clear who should have access to personal/sensitive information and that staff and managers understand their obligation and the security measures appropriate.

Sensitive data. Foster Care Link undertakes appropriate 'Safer Recruitment' practices relevant for staff who have access to client data. In particular as Foster Care Link has potentially sensitive data concerning vulnerable children and young people, employees are required to undergo DBS checks and this is repeated on a three-yearly basis. Any convictions are considered, and a decision reached as to whether this is detrimental to their continued position.

It is Foster Care Link's responsibility to ensure that the records and systems are backed up on a regular basis and to ensure that there is no loss or destruction of personal data accidentally. If employees are aware of any errors or have any concerns regarding personal data, this is be reported immediately to the identified Manager in this policy.

Staff have been trained and should have a clear understanding of practice and expectation including aspects such as:

- *who is appropriate to share information*
- *unauthorised access to or alteration, disclosure, or destruction of personal data*
- *accidental loss or destruction of personal data*
- *dealing with public enquiries*
- *establishing identity and entitlement of any person making enquiries before disclosing any information*
- *actions to be taken if doubts or concerns*
- *never discuss/disclose sensitive information to anyone unless sure they are an appropriate person to share and the client has given consent.*

Foster Care Link good practice principles for staff

- Never leave client records unattended or in such circumstances where third parties may gain access to them.

- Adopt and maintain a secure filing system and return client records to the filing system when not in use.
- Establish good practice guidelines regarding transportation of data particularly client hard copy records and IT memory sticks/CD/external hard drives/laptop, tape, disk, cassette/cartridge, hard drives, e.g. CD, DVD and ZIP drive

Requests for personal and client data held by MOU should immediately be sent to our data protection compliance officer Sarah Buglass.

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 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.

An individual is entitled:

- *to be informed whether personal data is held of which they are the subject*
- *to access any such data (may use Subject Access Requests, further information www.ico.org.uk or call ICO helpline 0303 123 1113)*
- *when appropriate, to have such data corrected or erased if there are no reasonable reasons as defined in the GDP Regulations for resisting such a request.*

Decision Making & Disposal

Data Controllers are responsible for the decision to dispose of data and retention period guidance.

Review should be conducted with the relevant stakeholders i.e. other Senior Managers, relevant external bodies (e.g. CQC, OFSTED), legal advisor, Markel.

The disposal decisions must be reached having regard for:

- *On-going business and accountability needs (including audit)*
- *Current applicable legislation*
- *Whether the record has any long term historical or research value*
- *Best practice in the applicable field*
- *Costs associated with continued storage verses costs of destruction*
- *The legal, political and reputational risks associated with keeping, destroying or losing control over the records.*
- *Could the data be returned to sender/provider to be stored e.g. Markel/client*

The decision to destroy should not be made with the intent of denying access or destroying evidence.

Additional notes

The agreed disposal decision should be recorded and retained including:

- *Description of the data/record*
- *Type of data (paper, IT)*
- *Creation date of record, review and decision date*
- *Disposal decision and method of disposal*
- *Summary of reasons for decision*

- *Names of people involved in decision*
- *Signature of person authorising disposal*

Destruction

To ensure compliance with the DPRegulations, all information, in any format, destroyed from any location must not expose confidentiality of our employees, clients and service users.

Additional notes
Foster Care Link has a procedure for the destruction of Confidential or Sensitive Waste paper base. It is local practice for all confidential information to be burned on site not shredded.

All office paper should be placed in confidential waste bins if the content is in any way sensitive. All other paper can be disposed of in the boxes or bins provided in offices.

Archiving

Data Controllers are responsible for the decision to retain records in accordance with the retention schedule.

Breaches of data

In the event of a potential, suspected or actual breach of data then the data controller or data processor at Foster Care Link must be notified immediately. Corrective actions will then be agreed in order to minimise the breach, inform the appropriate persons and take any actions required to correct such breach/s and ensure a repeat cannot happen.

Policy Review Date

The Registered Manager is responsible for regular review and updating of this policy.

References:
https://ico.org.uk/
www.acas.org.uk/
https://ico.org.uk/for-organisations/register/
https://ico.org.uk/media/about-the-ico/policies-and-procedures/1904/ico-retention-schedule.pdf