Data Protection

Version 2
2021
Review Date: 2023

Purpose of this policy

The Fostering Network is committed to complying with privacy and data protection laws, as outlined in the EU wide General Data Protection Regulation (GDPR), the UK Data Protection Bill once in force. This policy sets out what we do to protect individuals' personal information.

Anyone who handles personal data in any way on behalf of The Fostering Network, including employees, volunteers, consultants and suppliers must ensure they comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

This policy may be amended to reflect any further changes in legislation, regulatory guidance or internal policy decisions.

Brief introduction to Data Protection Act 1998

The Data Protection Act was established to make provision for the regulation of processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The act covers personal data relating to identifiable, living individuals. Data protection is about protecting individuals from the consequences of data being misused or handled badly, for example using data without the knowledge or wishes of the individual which could result in a breach of privacy.

There are certain exceptions where information may be disclosed without the knowledge or consent of the data subject. The Act states that Data Protection is not breached:

- If another law requires you to provide information, or
- If you choose to disclose information because not doing so would prejudice crime prevention, catching criminals or collecting taxes or duties.

Data Protection Principles

Below is a summary of The Data Protection Principles:

- Data 'processing' must be 'fair' and legal.
- You must obtain data only for specified purpose(s) and use it only in ways that are compatible with the purposes.
- Data must be adequate, relevant and not excessive.
- Data must be accurate and up to date.

- Data must not be held longer than necessary.
- Data Subjects' rights must be respected.
- You must have appropriate security.
- Special rules apply to transfers abroad.

Source: Lasa Guide to Data Protection

What is personal data?

For information to be 'personal' it must first relate to an identifiable, living, individual. It must also be about the person in some way i.e. contain some additional information about them rather than just mentioning them. The individual becomes 'identifiable' if you can work out who they are in any way e.g. by cross referencing sets of data.

- The definition of 'data' is quite broad. Data can be manual, held on computerised systems – including emails, spreadsheets and other documents as well as databases – or could be video information stored by a CCTV camera or photographs.

POLICY STATEMENT

The Fostering Network shall:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff who handle personal data, so that they can act confidently and consistently
- ensure appropriate technical security measures are in place
- maintain a register entry with the Information Commissioner on an annual basis, detailing the purposes for which it uses personal information
- comply with subject access requests within 40 calendar days, taking legal advice where appropriate

KEY RISKS

Three main areas of risk:

- safeguarding individuals from harm that could be caused by allowing their information to fall into the wrong hands, or by holding inaccurate or inappropriate data
- loss of data as a valuable commercial commodity
- damage to The Fostering Network's reputation

Some examples:

- Information about allegations that is inappropriately disclosed could cause personal distress to individual and / or have implications for legal proceedings
- Information about safeguarded families getting into the wrong hands could result in serious damage to the families
- Individuals could be harmed through data being inaccurate or insufficient, for example giving someone the wrong advice
- Loss of data through poor technical security measures, (e.g. lack of back-up routine, damage to server) could hamper our work with individuals, causing them harm as a result, would impact the whole organisation and would be costly to regain

RESPONSIBILITIES

Trustees

The board of trustees have overall responsibility for ensuring that the organisation complies with its legal obligations.

Data Protection Responsibilities – key member of staff

SLT has nominated the Director of Financial Resources as Data Protection Officer with the following responsibilities:

- brief the board / SLT on Data Protection responsibilities
- review Data Protection and related policies
- monitor compliance with the policy
- advise other staff on Data Protection issues
- notify the registry
- oversee subject access requests

Specific other staff

Key responsibilities held by other members of staff:

- Director of Communications and Public Affairs – responsible for approving Data-Protection-related statements on publicity materials, web etc.
- IT Systems and Database Manager – responsible for electronic security measures and database compliance with Data Protection Policy
- Facilities Manager – responsible for physical security of the London building

- People and Culture Manager - responsible for processing personal and sensitive data that relates to staff and others and ensuring that Data Protection induction and training takes place
- SLT – responsible for regular review of Data Protection policy and overseeing overall implementation
- Country Directors and Office Managers in Wales, Scotland & Northern Ireland – responsible for implementing Data Protection policy in their Country Offices

Team/Department managers

Each team or department where personal data is handled will be responsible for drawing up its own operational procedures in line with this policy to ensure that good Data Protection practice is established and followed.

Team managers must ensure that the Data Protection Officer is informed of any changes in their use of personal data that might affect the organisation's Notification.

Staff & volunteers

All staff, including volunteers are required to read, understand and accept the data protection policy and to follow established procedures that relate to the personal data they handle in the course of their work.

Enforcement

The Fostering Network requires all staff and volunteers to comply with the organisation's policies and procedures related to Data Protection. Failure to do so e.g unauthorised, inappropriate or excessive disclosure of information about individuals, or failure to follow security procedures, will be regarded as serious misconduct and will be dealt with in accordance with the organisation's disciplinary policy and procedure.

SECURITY

Setting Security measures

Below is a list of general security measures to protect personal data. Managers at all levels should assess the security levels needed for their data and then implement appropriate security measures to form their operational procedures. These should include – but are not restricted to – the measures listed below.

Physical security measures

- physical security of premises. Well lit exterior, good quality doors, locks and alarm system
- entry control including supervision of visitors
- clear desk policy
- disposing of paper waste containing personal information by shredding
- locking up laptops and other portable equipment including memory sticks and CDs
- regular system back ups to be stored in a separate location from main premises
- ensuring removal of personal information from old computers before disposal
- not taking member details or other confidential information externally unless for an agreed purpose approved by a line manager or in accordance with established working procedures.

Electronic security measures

- password protection, including password strength and preventing staff from sharing passwords
- control of access to certain parts of network
- encryption of files, memory sticks and CDs
- server security
- system security updates
- ensure firewall, virus protection and anti spyware is installed and up to date
- spam filters
- staff trained not to open spam email, to beware of phishing attacks and warned not to send emails that could put organisation in disrepute

Staff security measures

- check identity and reliability of staff at recruitment stage e.g. via references and checking of qualifications
- confidentiality agreement in employment contract stating what staff can and cannot do with personal information
- train staff about their responsibilities about the personal information they process, make clear what information is confidential and what the restrictions are for using it
- warn staff of dangers of ‘social engineering’ This is where people trick others into making disclosures of information
- clarify telephone procedures, can staff details be given out
- inform staff what personal use they can make of computers or phones

Contracts with third parties

- Ensure there are written contracts or full terms and conditions in place with any Data Processor (a third party handling personal information on behalf of The Fostering Network). These should be clear about the use and disclosure of the information. It should also require that they have in place equivalent security measures.
- A copy of all contracts with Data Processors must be passed to the Data Protection Officer, whose advice should be sought if in doubt.

Specific risks

HOME-BASED WORKERS:

Home-based workers should be careful to ensure that other household members cannot access to personal data as defined by data protection legislation.

To ensure confidentiality, it is important that appropriate security measures are put in place, in line with the BYOD policy.

STAFF WORKING AWAY FROM THE OFFICE:

Data taken outside of the office either in hard copy or electronic format carries an additional security risk. There is a higher risk of it being lost, stolen or a member of the general public obtaining unauthorised access, whether intentional or unintentional. Data should only be taken outside the office where there is an authorised reason and not if there is a viable alternative (such as accessing data remotely). Staff should take care to lock briefcases and laptops, encrypt files, and not leave personal information where it can be viewed by a member of the public.

DATA RECORDING AND STORAGE

Accuracy

Managers are required to consider whether additional measures need to be taken to ensure data accuracy. For example:

- when information is taken over the phone, how is it checked back with the individual?
- where information is supplied by a third party, what steps will be taken to ensure its accuracy
- is there a recording policy for your department?

Updating

Managers are required to define a regular cycle of checking, updating or discarding old data. See section below for retention periods which should be considered in relation to archiving practices.

Retention periods

All employees are required to comply with the Document Retention and Destruction Policy, to be found on the intranet.

SUBJECT ACCESS

Responsibility

The Data Protection Officer will be responsible for ensuring that subject access requests are handled within the legal time limit of 40 days.

Procedure for making request

Subject access requests must be in writing. Staff must notify their line manager of anything which might be a subject access request immediately upon receipt of request.

Legal advice will be sought where necessary.

Provision for verifying identity

Where the person managing the access procedure does not know the individual personally their identity must be checked before handing over any information.

Charging

There will be no charge to the Data Subject when they make an access request.

TRANSPARENCY

Commitment

The Fostering Network endeavours to make data subjects aware that their data is being processed and

- the purposes it is being processed for
- what types of disclosure are likely, and
- how to exercise their rights in relation to the data

Procedure

Data subjects will be informed of this commitment via:

- staff handbook
- induction procedure
- membership application and other data capture forms
- during the initial interview with service users
- on the web site including intranet
- public register with Information Commissioner

CONSENT AND MARKETING

In most cases The Fostering Network will obtain consent for processing personal data, in order to comply with the Fair Processing Conditions (see notes). This consent may be verbal or written, depending on how the information is obtained.

Where appropriate, data may also be processed without consent, on the basis of one of the five other Conditions.

The Fostering Network acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time (for example to meet statutory requirements), even though consent for using it has been withdrawn.

Disclosure

The Fostering Network may disclose data without seeking consent if there are over-riding reasons, and in particular where a child's welfare may be at risk. Please see The Fostering Network Child Protection Policy for further information.

Direct marketing

Guidance from the Information Commissioner's Office suggests that most unsolicited direct contact with individuals should be treated as marketing. This includes seeking donations, marketing goods and services, promoting sponsored events, raffles, etc.

Data Subjects have the right to require their data not to be used for marketing; therefore the Fostering Network will make it clear when there is an intention to use their data for marketing purposes.

Data Subjects will be offered an opt-out (via a tick-box or an easy-to use alternative) where appropriate. These preferences must be recorded via the CRM system.

The current practice is not to share or exchange lists with other organisations in order to carry out marketing activities. However should this practice be reviewed in future Data Subjects will be given an opt-out from their details being shared.

Where a list is purchased externally it must be guaranteed that those on the list have been given an opportunity to opt out, and that the list is sufficiently up to date.

Because of the Privacy and Electronic Communications (EC Directive) Regulations 2003 most electronic marketing (by phone, fax, e-mail or text message) either requires consent in advance, or it is good practice to obtain consent. Detailed policies in this area are the responsibility of the fundraising team.

STAFF TRAINING & ACCEPTANCE OF RESPONSIBILITIES

Documentation

The Fostering Network Data Protection Policy will be the main policy document for the organisation. Team and department managers will document operational procedures based on an understanding of the main policy document, seeking guidance from the Data Protection Officer where needed. This policy should be read in conjunction with the Fostering Network Child Protection Policy and the Employee Data Policy and Procedure.

Useful websites

- The Information Commissioner, helpline no: 0303 123 1113

Induction

All staff will be inducted on their responsibilities under the policy when they join the organisation and during department training. Team managers will be made aware of their responsibility in this area by the Data Protection Officer / Senior Management Team

Continuing training

General training on data protection will be carried out at regular stages. Data Protection issues can also be raised and reviewed during team meetings, supervisions, etc

Procedure for staff signifying acceptance of policy

Staff and volunteers must read and sign the policy as part of their induction to the organisation. Line managers will be responsible for drawing up operational procedures by department and to ensure their team understand these measures and comply with them.

I confirm that I have read and understand the above policy:

Signed…… Date…….

GENERAL NOTES

Data Controller

The Data Controller is the legal 'person' responsible for complying with the Data Protection Act. It will almost always be the organisation, not an individual staff member or volunteer. This means that The Fostering Network retains responsibility, even where data is being processed by remote workers, volunteers and national offices.

Separate organisations (for example a charity and its trading company) are separate Data Controllers. Where organisations work in close partnership it may not be easy to identify the Data Controller. If in doubt, seek guidance from the Information Commissioner.

Data Processor

When work is outsourced, which involves the contracting organisation in having access to personal data, there must be a suitable written contract in place, paying particular attention to security. The Data Controller remains responsible for any breach of Data Protection brought about by the Data Processor.

Fair processing conditions

Schedule 2 of the Data Protection Act lays down six conditions, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

- With consent of the Data Subject
- If it is necessary for a contract involving the Data Subject
- To meet a legal obligation
- To protect the Data Subject's 'vital interests'
- In connection with government or other public functions
- In the Data Controller's 'legitimate interests' provided the Data Subject's interests are not infringed

Notification

The Data Protection Officer maintains The Fostering Network's entry on the Information Commissioner's register, describing in broad outline the types of data processed and the purposes for which it is used.

Subject access

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request (including the fee, if required), the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld. This includes some third party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)