Jade Mutua Foundation Trust

Data Protection Policy

Contents

Jade Mutua Foundation Trust

Data Protection Policy

1. Data protection principles

The *(put name of your organisation)* is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

a. This policy applies to all personal data processed by the *(put name of your organisation)* .
b. The Responsible Person and will take responsibility for the *(put name of your organisation)* ongoing compliance with this policy.
c. This policy will be reviewed at least annually.
d. The *(put name of your organisation)* is exempt from having to register with the Information Commissioner's Office but can do so voluntarily if deemed helpful by the trustees or advised by the person responsible for data processing.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the *(put name of your organisation)* will maintain a Register of Systems.

b. The Register of Systems will be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the ***(put name of your organisation)*** will be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the ***(put name of your organisation)*** is done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests
b. The ***(put name of your organisation)*** notes the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent is kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent is clearly available and systems should be in place to ensure such revocation is reflected accurately in the ***(put name of your organisation)*** systems.

5. Data minimisation

a. The ***(put name of your organisation)*** ensures that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. Personal data may include permission for use of image or personal details for promotional purposes; this may be revoked by an individual at any time.

6. Accuracy

a. The ***(put name of your organisation)*** takes all reasonable steps to ensure personal data is accurate.
b. Steps are in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the (***put name of your organisation)*** operates an archiving procedure for each area in which personal data is processed and implements this procedure annually.
b. Archiving decisions consider what data should/must be retained, for how long, and why.

8. Security

a. The ***(put name of your organisation)*** ensures that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data is limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information.
c. When personal data is deleted this will be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions are in place.

Jade Mutua Foundation Trust

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the ***(put name of your organisation)*** will promptly assess the risk to people's rights and freedoms and, if appropriate, report this breach to the ICO. (See document Data protection Breach Response Procedure).

End of policy

(put name of your organisation) **(Check below what applies to your organisation)**

REGISTER OF SYSTEMS FOR PERSONAL DATA

1. Members

a. Database – electronic – Google Drive – restricted access
b. Files – electronic – Google Drive – restricted access
c. Files – hard copy, office filing cabinet – restricted access by key
d. Email records – electronic – office and managers' computers – restricted access by password

Documents Database list; application forms; assessments; consent forms

Contents Name; date of birth; address; telephone numbers; email address; carer/parent details

Function i, ii, iii, vii

2. Parents & Carers

a. Database – electronic – Google Drive
b. Email records – electronic – office and managers' computers – restricted access by password
c. Members files – hard copy, office filing cabinet – restricted access by key

Documents Database list; member application forms; email lists

Contents Names; address; telephone numbers; email address; email records

Function i, ii, vii

3. Staff & Volunteers

a. Database – electronic – Google Drive
b. Files – electronic – Managers' computers – restricted access by password
c. Files – hard copy – office filing cabinet – access by keys restricted to managers

Documents Database list; application forms; new staff details form; payment details; supervision and appraisal recordings; recordings under policies, e.g. disciplinary, grievance; letters, emails; references; contract of employment; DBS results forms

Jade Mutua Foundation Trust

Contents Recruitment and general communications; performance; names; address; email address; telephone numbers; application information; outcome of DBS checks

Function i, ii, iii, vii

4. General

4.1 Stakeholders: donors; partner agencies; community groups/individuals

4.2 Funding bodies

4.3 Centre users; general public

a. Accident reports – hard copy, office locked cupboard – staff access only by key
b. Safeguarding reports – recordings in member files – electronic and office (as above)
c. Letters or emails – electronic – office and Managers' and trustee computers – restricted access by password

Lawful purposes for all above data processing systems A. B. D. F. (see key below).
Types of data processing

i. Conversion converting data to another format.
ii. Validation – Ensuring that supplied data is clear, correct and useful.
iii. Sorting – Arranging items in some sequence and/or in different sets.
iv. Summarisation – Reducing detail data to its main points.
v. Aggregation – Combining multiple pieces of data.
vi. Analysis – The collection, organisation, analysis, interpretation and presentation of data.
vii. Reporting – Listed detail or summary data.

Lawful basis for data processing

A. Consent
B. Contract
C. Legal obligation
D. Vital interests
E. Public task
F. Legitimate interests

Guidance for staff, trustees and volunteers

Also see: Information, Technology & Communications Policy – Staff Handbook
Safeguarding and Confidentiality policies and procedures

1. Keep secure all files containing personal data whether on paper or on computer.
2. All paper based personal information should be locked away at night whenever it is not being accessed – in particular, consider paperwork left on desks

3. Laptops, other portable equipment containing personal data, computer media like discs or memory sticks should be inaccessible except to authorised personnel – use passwords and check security when communicating with others.
4. Email attachments (e.g. spreadsheets) containing personal data should be password protected and the password sent to the recipient in a separate email.
5. Ensure all data/information is stored securely and revealed only to those members of staff who need to know it.
6. Any personal data held on portable media, and allocated laptops must be encrypted/password protected**.**
7. A member of staff should be responsible for checking at least annually that personal data in personal files is up to date and accurate and any unnecessary documents destroyed.
8. Confidential waste must always be shredded, and not put into a waste or recycling bin.

HOW TO PREPARE FOR GDPR AND DATA PROTECTION REFORM

1 **Make sure the right people in your organisation know this is coming**

Your trustee board and senior staff should be aware that the law is changing. They need to know enough to make good decisions about what you need to do to implement GDPR. They need to be aware that implementation may take considerable time and effort and add data protection to your risk register if you have one.

2 **Identify what data you hold and where that data came from**

If you don't know what personal data you hold and where it came from you will need to organise an audit of your different systems and departments to find out. This means all personal data including employees and volunteers, service users, members, donors and supporters and more. You should document your findings as GDPR means you must keep records of your processing activities. You should also record if you share data with any third parties.

3 **Update your privacy notices**

You must always tell people in a concise, easy to understand way how you intend to use their data. Privacy notices are the most common way to do this. You may well already have privacy notices on your website for example, but they will all need to be updated. Under GDPR privacy notices must give additional information such as how long you will keep data for and what lawful basis you have to process data

4 **Check your processes meet individuals' new rights**

GDPR will give people more rights over their data. For example, GDPR gives someone the right to have their personal data deleted. Would you be able to find the relevant data and who would be responsible for making sure that happened? **Get to know the eight rights** and have the systems in place to be able to deliver on each of them.

Jade Mutua Foundation Trust

5 **Know how you will deal with 'subject access requests'**

Individuals have the right to know what data you hold on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form (hard copy). This is known as a subject access request. Your organisation needs to be able to identify a subject access request, find all the relevant data and comply within one month of receipt of the request.

6 **Identify and document your 'lawful basis' for processing data**

To legally process data under GDPR you must have a 'lawful basis' to do so. For example, it is a lawful basis to process personal data to deliver a contract you have with an individual. There are a number of different criteria that give you lawful basis to process and crucially, different lawful bases give different right to individuals. For example, if you rely on consent as a lawful basis, individuals have stronger rights to have their data deleted. Understand and document what lawful basis you have to process data.

7 **Review how you get consent to use personal data**

If you rely on consent as your lawful basis for processing personal data, then you need to review how you seek and manage consent. Under GDPR consent must be freely given, specific and easily withdrawn. You can't rely on pre-ticked boxes, silence or inactivity to gain consent instead people must positively opt-in.

8 **Build in extra protection for children**

Many charities support children and young people and GDPR brings in special protection for children's personal data. GDPR says children under 16 cannot give consent (although this may be reduced to 13 in the UK) so you may have to seek consent from a parent or guardian. You will need to be able to verify that person giving consent on behalf of a child is allowed to do so and any privacy statements will need to be written in language that children can understand.

9 **Get ready to detect, report and investigate personal data breaches**

A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. You will need to have the right procedures in place to detect, investigate and report a personal data breach. GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned. You need to be able to demonstrate that you have appropriate technical and organisational measures in place to protect against a data breach.

10 **Build data protection into your new projects**

Privacy by design means building data protection into all your new projects and services. It has always been good practice, but GDPR makes privacy by design an express legal requirement. To achieve this, data protection impact assessments should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or sensitive categories of data will be processed on a large scale. Clarify who will be responsible for carrying out impact assessments, when you will use them and how you will record them.

11 **Decide who will be responsible for data protection in your organisation**

Someone in your organisation, or an external data protection advisor, has to take responsibility

for compliance with data protection legislation and have the knowledge and authority to do this effectively. Some organisations will need formally appoint a data protection officer (DPO) for example if you organisation carries out large scale processing of sensitive personal data such as health records or information about criminal convictions.

12 **Get up to speed on data protection and fundraising**

The use of personal data is central to most fundraising activities and there has been a great deal of public and media scrutiny of fundraising techniques. If you use personal data to fundraise then you need to follow the latest guidance on fundraising and data protection.

The GDPR provides the following rights for individuals:

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

Updated 2018