Oxfordshire Family Support Network

DATA PROTECTION POLICY - FINAL

Introduction

OxFSN (Oxfordshire Family Support Network) needs to gather and use certain information about individuals.

These can include people we support such as family carers, and their family members, employees, volunteers, donors and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet OxFSN's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures OxFSN:

- Complies with data protection law and follows good practice
- Protects the rights of staff, the people we support employees, volunteers, donors and other people the organisation has a relationship with or may need to contact
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulations 2018 or GDPR describe how organisations - including OxFSN - must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by six important principles. These say that personal data must:

1. Be processed lawfully, fairly and transparently
2. Can only be collected for specified, explicit and legitimate purposes
3. Be adequate, relevant and limited to what is necessary for processing
4. Be accurate and kept up-to-date
5. Be kept in a form such that the data subject can be identified only as long as is necessary for processing
6. Be processed in a manner that ensures security

The Definition of Personal Data

The definition of personal data in the GDPR is broadened to include 'any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.'

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of OxFSN
- All staff, contractors and volunteers of OxFSN
- All suppliers and other people working on behalf of OxFSN

It applies to all data that OxFSN holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect OxFSN from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how OxFSN uses data relating to them.
- **Reputational damage.** For instance, OxFSN could suffer if hackers successfully gained access to sensitive data.

- **Administrative Penalty for Infringement of Articles.** Dependant on which article is infringed; the penalty can be up to 4% of annual global turnover or €20 million, whichever is greater.

Responsibilities

Everyone who works for or with OxFSN has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and the GDPR principles.

However, these people have key areas of responsibility:

- The **Board of Trustee** is ultimately responsible for ensuring that OxFSN meets its legal obligations.

- The **Data Protection Officer, Gail Hanrahan,** is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Style Acre holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **IT contractor,** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The **Project Officer, Angeli Vaid,** is responsible for:

- Approving any GDPR statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by GDPR principles.

- The data controllers (in this case OxFSN, Data Protection Manager) are responsible for:

- Carrying out Data Protection Impact Assessments for technologies and processes that are likely to result in a high risk to the rights of data subjects

The **data processors** (OXFSN, employees and contractors) are responsible for:

- Keeping a record of all processing carried out on behalf of the data controller

Rights of the Data Subject

The GDPR give data subjects the following rights:

- OxFSN must be clear about what data it is collecting about data subjects and why
- Data subjects must give explicit and clear consent – it can no longer be implied
- Processing cannot proceed until consent has been given for every processing activity
- There needs to be a clear process for how consent can be withdrawn*
- Data subjects have the right to be forgotten and any data held about them erased**

*OxFSN must stop processing the data subject's personal data unless:

- It can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims

**OxFSN can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- The exercise or defence of legal claims

Article 6.1 of the GDPR defines the lawful grounds for data processing as follows:

1. Consent of the data subject
2. Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

3. Processing is necessary for compliance with a legal obligation
4. Processing is necessary to protect the vital interests of a data subject or another person
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6. Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)

OxFSN ensures that individuals are aware that their data is being processed and they understand:

- How the data is being used
- How to exercise their rights

All data subjects are asked to consent to their data being processed. Consent is obtained for each process prior to commencement. There is also a clear procedure for withdrawing consent, documented on the consent form itself.

For staff and the people we support, the vast majority of the personal data that is stored and processed by OxFSN is done so to enable the individual to work for/be supported by the charity. Although consent is asked for there are many situations that an individual cannot refuse/withdraw consent/request erasure due to the reasons permitted under Article 6.1 of the GDPR, namely point 2 and 4 above.

If this is the case OxFSN will write to the individual to explain the reason why their refusal/withdrawal of consent/request for erasure cannot be granted.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **OxFSN will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.

- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from the Data Protection Officer if they are unsure about any aspect of data protection.

Data storage

The GDPR requirements:

- Data to be stored with confidentiality and integrity secured including measures taken against accidental loss, destruction or damage
- Article 30 requires every data controller to retain a record of data processing activities. This must contain a specific set of information so it is clear what is being processed, where it is processed, how it is processed and why it is processed
- Data processors are required to keep a record of all processing carried out on behalf of the data controller

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data only of value to OxFSN when the charity can make use of it. However, it is when personal data is accessed and used that it can also be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**.
- Data must be **encrypted before being transferred electronically**. Contact your manager if you are unsure how to do this.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy

The law requires OxFSN to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all OxFSN, staff, contractors and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.**
- OxFSN will make it **easy for data subjects to update the information** OxFSN holds about them.
- Data should be **updated as inaccuracies are discovered**.

Subject access requests

All individuals who are the subject of personal data held by OxFSN are entitled to:

- Ask **what information** the charity holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how OxFSN is **meeting its GDPR obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at gail.hanrahan@oxfsn.org.uk. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 30 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Processing via a Third Party

Where a data controller contracts with a data processor to process personal data, that processor must be able to provide 'sufficient guarantees to implement appropriate technical and organisational measures that processing will comply with the GDPR and ensure data subject's rights are protected.

Data responsibilities will be documented very clearly to ensure there is no confusion.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, OxFSN will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the charity's legal advisers where necessary.

Reporting Data Breaches

Data breaches must be reported to the supervisory authority (ICO) and the data subjects which they affect.

- Data breach reports must be made within 72 hours of the breach
- Data breaches must be reported to the Data Protection Officer

- Data breaches are to be reported via an incident form which must include measures being taken to address the breach and mitigate any possible side effects

Date: 8 May 2018

This Policy will be reviewed every 3 years