youth focus NW
Improving the lives of young people

Policy Title	YFNW Data Protection Policy Version 2.0
Author	Youth Focus NW
Approved by	The Board of Trustees
Audience	• Staff team, • Board of Trustees, • Sessional workers, • Volunteers and Service Users
Release date	July 2000
Review date	July 2022 - reviewed Next review date July 2024
References	https://ico.org.uk/

Contents: **Page no:**

Introduction

Youth Focus NW (YFNW) is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

Youth Focus NW needs to collect and use certain types of information about the Data Subjects who come into contact with us in order to carry out our work. This personal information must be collected and dealt with appropriately and there are safeguards to ensure this under the General Data Protection Regulation May 2018.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work.

Definitions

Charity purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and project development purposes. *Charity purposes include the following:* - *Compliance with our legal, regulatory and charitable governance obligations and good practice* - *Ensuring charity policies are adhered to* - *Operational reasons, such as obtaining consent for young people's activities, safeguarding, evaluation and monitoring equality and diversity* - *Investigating complaints and incidents* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Reviewing and Improving services*

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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 that natural person. *Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, age, religion and gender.*
Special categories of personal data	Special categories of data include information about an individual's age, racial or ethnic origin, sexual orientation, gender, religious or similar beliefs, physical or mental health or condition, criminal offences, or related proceedings —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is [the Information Commissioner's Office - ICO].

The principles

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Youth Focus NW shall comply with the principles of data protection enumerated in the EU General Data Protection Regulation. We will make every effort possible to comply with these principles. The Principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Purpose Limitation

Data can only be collected for a specific purpose.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accuracy

The data we hold must be accurate and kept up to date.

5. Storage Limitation

We cannot store data longer than necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

7. Accountability

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. We are all responsible for understanding our own particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments where appropriate
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased immediately.

Lawful basis for processing data

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose, i.e Youth Voice activities

2. **Contract**

The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation**

We have a legal obligation to process the data (excluding a contract).

4. **Vital interests**

Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public function**

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest**

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- ethnic origin
- gender

- religion
- health/ability
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. in the event of a safeguarding issue). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Responsibilities

Organisational responsibilities

- Analysing and documenting the type of personal data we hold and the justification for holding that data
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are clear and lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Staff responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay
- Undergo data protection training
- Check security of portable devices, do not use an unsecured wifi if working remotely. Do not use any personal device for work purposes.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DESIGNATED OFFICER will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- Data on paper is discouraged, if unavoidable it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be encrypted or held on a secure drive. All laptops and personnel files will be encrypted
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones unless using encrypted software.
- Consents and personal data is held on a secure CMS
- Shared files are online, there is no server or back up.
- All possible technical measures must be put in place to keep data secure
- Use of pen drives/USBs are discouraged and in no circumstances will staff use a strange device.
- Electronic data will not be kept longer than necessary and deleted once no longer needed.

Data retention

We must not retain personal data for longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Any removal of data is secure - paper copies are shredded and electronic data is deleted from our system. We have recently removed our ‘server’ meaning we have no back up of files and all is held on a secure gdrive accessed via encrypted devices.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the designated officer.

Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month.

4. Right to erasure

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and/or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation

We can only refuse to comply with a right to erasure in the following circumstances:

- 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, eg safeguarding
- For public health purposes in the public interest

- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims and investigations

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy notices

Example - Networks

Youth Focus NW is a Charitable Company Limited by Guarantee and is governed by a Board of Trustees. This privacy policy explains how we use any contact information we collect about you when you join any of our networks or participate in our events.

Youth Focus NW is a strategic organisation that creates networking opportunities for professionals working with young people. We need to collect contact information in order to carry out our work. This information must be collected and dealt with appropriately and there are safeguards to ensure this under the General Data Protection Regulation May 2018.

Why do we collect your data?

- We collect your contact details which may include email, contact address & number in order to keep our networks relevant and up to date. Where possible we will collect contact information that is in the public domain (for example Local Authority email addresses). However, it is sometimes necessary to collect personal contact information and we will keep this to a minimum.
- We will use your information to send you relevant information on policy and practice to support your work together with networking opportunities we believe would be of benefit to you.

How do we collect your data?

- A data collection process or consultation
- When attending meetings and events
- You may contact us to ask us to add you to a mailing list or newsletter
- We will treat your data with the utmost care and take steps to protect it.

When will we share your information?

There may be a justified reason to share your information or you may request that we put you in contact with other professionals in order to benefit your work. We will only share your information when permission to do so has been granted.

When necessary we will share your information with third parties if funding contracts require it. In this instance we will ensure that your information is not shared further by implementing agreements with the relevant third parties. You can ask to see such agreements by emailing s.watts@youthfocusnw.org.uk with the heading **'GDPR Agreement request'**

Access to your information and correction:

You have the right to request a copy of the information that we hold about you. If you would like a copy please email s.watts@youthfocusnw.org.uk with the heading **'GDPR Information Request'**

We want to make sure that your contact information is accurate and up to date. You may ask us to correct or remove information you think is inaccurate. We would appreciate your support in informing us if you move on, change contact details etc

You have the right to remove your information and leave our networks at any time by emailing s.watts@youthfocusnw.org.uk with the heading **'GDPR - I want to opt out'**

How long will we keep your information?

We will review our network information on an annual basis and will not keep any information longer than necessary. Should a network cease, we will delete that mailing list.

Third parties

As a data controller we must have data sharing agreements in place with any third party [data controllers (and/or) data processors] that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

[For controllers] As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

[For processors] As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Agreements

Agreements must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with [data controllers (and/or) data processors] must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our agreements must include:

- Acting only on written instructions and/or consent given
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments

- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

Criminal offence data

- Any criminal record checks are justified by law.
- All staff working directly with children and young people are subject to an enhanced DBS check.

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. Youth Focus NW has a legal obligation to report any data breaches to ICO within 72 hours of becoming aware of the breach.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Business Development Manager of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Failure to comply

- We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.
- The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.
- If you have any questions or concerns about anything in this policy, do not hesitate to contact the Business Manager