YOUNGROOTS
Supporting young refugees

Data Protection Policy

Introduction

The General Data Protection Regulation (GDPR), came into force on the 25th May 2018, and regulates the processing of personal data, and protects the rights and privacy of all individuals (including children). It describes how organisations must collect, handle, and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

The GDPR places responsibility on organisations to process any personal data in accordance with the following eight principles:

1. Be processed fairly and lawfully;
2. Be obtained only for specific, lawful purposes;
3. Be adequate, relevant, and not excessive;
4. Be accurate and kept up to date;
5. Not be held for any longer than necessary;
6. Processed in accordance with the rights of data subjects;
7. Be protected in appropriate ways; and
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

This new regulatory environment demands higher transparency and accountability in how organisations manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use. To comply with the law, organisations must ensure that personal information is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Given the work that it undertakes, it is necessary for Young Roots to gather and use certain information about individuals. This includes personal information about the young people who use the services of Young Roots and the supporters of the organisation, as well as Young Roots' employees. Young Roots is committed to a policy of protecting the rights and privacy of individuals, in accordance with GDPR.

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

Purpose of policy

This data protection policy ensures that Young Roots:

- Complies with data protection law and follows best practice
- Protects the rights of staff, volunteers, supporters and the young people it serves
- Exhibits transparency in how it stores and processes individuals' data
- Protects itself from the risks of data breach

Types of Data

As data controller, Young Roots will process personal data, including data that falls under the special category, for its 'employees' (which refers to both paid staff and volunteers), its young people, and its supporters. The following sets out the types of data that Young Roots may obtain from each group of data subjects.

Employees[1]

Young Roots collects a range of information about you. This includes:

- your name, address and contact details, including email address and
- telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration,
- whether or not you have a disability for which the college needs to make
- reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your
- ethnic origin, sexual orientation, health, and religion or belief.

Young Roots collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

Young Roots will also collect personal data about employees from third parties, such as references supplied by former employers, information from employment background check providers, and information from criminal records checks. Young Roots will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application

[1] 'Employee' refers to both paid staff and volunteers.

record, in HR management systems and on other IT systems (including email Data about employees may be processed for legal, personnel, administrative and management purposes and to enable Young Roots to meet its legal obligations as an employer (e.g. to pay employees, monitor their performance, and to confer benefits in connection with their employment). Young Roots may be required to process sensitive personal data of employees, including the following:

- An employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;
- An employee's racial, ethnic origin, religious and/or similar information in order to monitor compliance with equal opportunities legislation; and/or
- Any other relevant sensitive personal information in order to comply with legal requirements and obligations to third parties.

For further information on why Young Roots processes employee's personal details and who has access to data, how Young Roots protects its data, and for how long Young Roots keeps employee data please refer to our privacy notice.

Young People

Young Roots provides support to a population of young people who are classified as vulnerable. As such, it is particularly important that their personal data is handled appropriately (see Key Risks as related to young people). Data about young people may be processed to enable Young Roots to deliver a careful and well-targeted service to them. Young Roots may be required to process sensitive personal data of young people, including the following:

- A young person's physical or mental health or condition in order to provide the young person with support or access to other services;
- A young person's racial, ethnic origin, religious and/or similar information in order to monitor compliance with equal opportunities legislation, report to funders, and ensure that services are provided in a manner which is meets the needs of these characteristics; and/or
- Any other relevant sensitive personal information in order to comply with legal requirements and obligations to third parties.

Supporters

Data about our supporters, including funders, may be processed to enable Young Roots to keep them updated with the progress of the organisation and to help seek additional funding. It is unlikely that we will hold sensitive personal data about our supporters. Supporters will be given a choice to opt-out of communications from Young Roots.

Young Roots will obtain the data subject's explicit consent to the processing of personal data, particularly data that is deemed sensitive.

Policy Statement

Young Roots is committed to a policy of protecting the rights and privacy of individuals, including the young people it serves and the supporters of the organisations, in accordance with GDPR. Specifically, Young Roots commits to:

- Comply with both the law and best practice
- Respect the rights of individuals (including employees, young people, and supporters)
- Be open and honest with individuals whose data is held by Young Roots
- Provide training and support to employees who handle personal data, so that they can act confidently and consistently
- Notify the Information Commissioner voluntarily, even if this is not required[2]

Please note that individual's rights have changed under GDPR[3]. These include the following eight rights:

1. Right to be informed
2. Right to access
3. Right to rectification
4. Right to erasure
5. Right to restrict
6. Right to portability
7. Right to object
8. Right not to be subject to automated decision-making

Key Risks

This data protection policy helps to protect Young Roots from data security risks, including:

- **Breaches of confidentiality**, whether through poor security or inappropriate disclosure of information;
- **Damage to the individual**, where the breach of sensitive personal information could pose a threat to the safety/security of an individual[4];
- **Failing to offer choice**, where individuals do not have the freedom to choose how Young Roots uses data related to them; and/or
- **Reputational damage**, where Young Roots would suffer if a data breach where to occur.

Responsibilities

---

[2] Guidance on when breaches should be reported can be found on the Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personaldata-breaches/

[3] Further information on individuals' rights can be found on the Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ [4] This is especially relevant to the young people served by Young Roots, who are considered vulnerable children and adults.

Everyone who works for or with Young Roots has some responsibility for ensuring that personal data is collected, stored, and handled in line with this data protection policy and in compliance with the law. This section outlines the specific responsibilities of Young Roots employees at each level of the organisation.

The Board of Trustees

The Board of Trustees has overall responsibility for ensuring that Young Roots complies with its legal obligations under GDPR. All members of the Board will undertake training on data protection. The Board will review and approve Young Roots' data protection policy every two years.

Data Protection Officer

The Data Protection Officer will be responsible for the following:

- Briefing the Board on data protection responsibilities
- Reviewing data protection and related policies (every two years)
- Advising staff and volunteers on tricky data protection issues
- Ensuring that data protection induction and training takes place
- Notifying the ICO of any breaches in data protection
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts or agreements with third party data processers that may handle Young Roots' sensitive data (where applicable)

The Data Protection Officer will be a member of the Board of Trustees.

The Director

The Director of Young Roots will support the Data Protection Officer and the Board to ensure that Young Roots is compliant with data protection law.

Employees

All employees are required to read, understand, and accept the policies and procedures related to the personal data they may handle in the course of their work.

Enforcement of responsibilities

Any breach of the data protection policy will be taken seriously and may result in disciplinary action.

Security

Young Roots will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

Procedures to ensure data security include:

- **Entry controls**. Only authorised persons will have access to office areas. Any stranger seen in office areas should be reported.
- **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal**. Paper documents should be shredded. Removable devices (i.e. CDs or USB flash drives) should be physically destroyed when they are no longer required.
- **Equipment**. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended. Data users wishing to use their own device must adhere to Young Roots' 'Bring Your Own Device' policy (as outlined in the Employee Handbook and the 'Data Protection in Practice' guide).

Risk assessments will be completed periodically by the Director and the Data Protection Officer to ensure that security measures remain appropriate and up to date. Where no longer appropriate, security measures will be changed; updated measures will be communicated to employees and implemented within a reasonable amount of time. Data recording and storage

Accuracy

The law requires that Young Roots take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. These guidelines should be followed to ensure the data accuracy: • Data will be held in **as few places as necessary**, where possible only in Lamplight.

Unnecessary additional data sets should not be created.

- Employees should take **every opportunity to ensure data is updated**.
- Young Roots will make it **easy for data subjects to update the information** Young Roots holds on them.
- *Data will be updated as inaccuracies are*

discovered. Updating

Data will be regularly reviewed and updated if it is found to be out of date. Changes to data will be made directly in Lamplight, the database system used by Young Roots. Old data will be deleted and disposed of from Lamplight in accordance GDPR good practice.

Storage

When data is **stored on paper**[4], it will be kept in a secure place where unauthorised people cannot see it. These guidelines should be followed for data stored on paper:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure that paper or 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**[5], it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts. These guidelines should be followed for data stored electronically:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable devices** (i.e. USB flash drive), these should be kept locked away securely when not being used.
- Data should only be stored on **Lamplight** (i.e. designated database system) and should only be uploaded to an **approved cloud computing service**.
- Data should **never be saved directly** to laptops or other mobile devices such as tablets or smart phones.
- All computers containing data should be protected by an **approved security software**.

Right to Access

All individuals who are subjects of personal data held by Young Roots are entitled to:

[4] This also refers to data that is usually stored electronically but has been printed.

[5] Please note that Young Roots uses Lamplight to store data centrally and securely.

- Ask **what information** Young Roots holds about them and why;
- Ask **how to gain access** to this information;
- *Be informed how to keep it up to date; and*
- Be informed how Young Roots is **meeting its data protection obligations**.

If an individual contacts Young Roots requesting this information, this is called a **Subject Access Request**.

Subject Access Requests should be made formally in writing, addressed to the Data Protection Officer at london@youngroots.org.uk.

Individuals will be charged £10 per subject access request. The Data Protection Officer will aim to provide the relevant data within 30 working days of the request and will verify the identity of data subject before personal information is provided.

Lawful Basis

Young Roots aims to ensure that individuals are aware that their data is being processed, and that they understand:

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

To these ends, Young Roots has a specific privacy notice for each of its data subjects (namely its employees, its young people, and its supporters). These privacy notices set out how data relating to the individual is used and includes information on opting out and withdrawing consent.

These privacy notices are available on request, and a version of this statement is also available on the Young Roots website.

Employee Training and acceptance of responsibilities

Training on data protection will be provided to all employees and members of the Board during the induction process. This will include practical guidance on how to ensure adherence to data protection policies (as outlined in the accompanying ‘Data Protection in Practice’ guide). This data protection policy will also be included in the Employee and Board Handbooks.

Employees should raise immediate data protection issues with their line manager or with the Data Protection Officer. They will have the opportunity to raise data protection issues during regular team meetings, and continued training will be provided to employees regularly.

Policy Review

Young Roots will review its data protection policy every 2 years. The Data Protection Officer will undertake this process, with the assistance of the Director. The Board of Trustees must approve the reviewed and updated policy. All employees will be made aware of any changes to the data protection policy within one month of its approval by the Board.

Data Retention

Category of personal data	**Period for which data is retained**
Basic personal information and contact details (including name, address, date of birth, gender, telephone number, email address and next of kin/ emergency contact details)	Existing employees: throughout their employment Unsuccessful applicants: 6 months Former employees: 6 years
Recruitment records (including CVs, application forms, interview notes, test results, proof of right to work in UK (such as passports and visas), driving license, evidence of skills and qualifications, and references)	Existing employees: throughout their employment Unsuccessful applicants: 6 months Former employees: 6 years
a) If someone volunteered with us and then applied for a paid role but was unsuccessful b) If someone has been unsuccessful in one round of recruitment but then applies for and gets another role c) If a current staff member applies for another role within the organisation and is unsuccessful	Keep recruitment records for 6 years (previous employee / volunteer) If less than 6 months has passed and we still have the recruitment records of the first application, keep these as part of the employees record Keep recruitment records relating to the unsuccessful application as part of their staff file
Offer letters, contracts of employment, written statements of terms and related correspondence	Existing employees: throughout their employment Former employees: 6 years
Financial and tax information (including pay and benefit entitlements, bank details and national insurance numbers)	Existing employees: throughout their employment Former employees: 7 years
Disciplinary and grievance records (including records of investigations, notes of disciplinary or grievance meetings and appeal hearings, correspondence with employees and written warnings)	Existing employees: for the period that the warning was live. Former employees: 6 years

Absence and leave records containing special categories of personal data (including details of absence or leave taken, the reasons for absences, the type of leave, information about medical or health conditions, reasonable adjustments, records of absence management discussions, correspondence with employees and written warnings)	Existing employees: throughout their employment. Former employees: 6 years. Can keep for longer if industrial accident.
Performance records (including appraisal documents, performance reviews and ratings, targets and objectives, performance improvement plans, records of performance improvement meetings and related correspondence, and warnings)	Existing employees: throughout their employment Former employees: 6 years
Termination of employment documentation including resignation letters, exit interviews, settlement agreements, dismissal letters, redundancy letters and any other associated documentation.	Existing employees: throughout their employment Former employees: 6 years