Data Protection policy

Youth Initiatives (YI) takes the security and privacy of your data seriously. We need to gather and use certain information about individuals. These can include young people, parents, donors, employees and other people the organisation has a relationship with or may need to contact. It is the policy of Youth Initiatives to collect, handle and store personal data in a way that:

- Complies with data protection law and follows good practice i.e EU General Data Protection Regulation (GDPR)
- Protects the rights of staff, young people, donors and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Youth Initiatives undertakes to comply with the requirements of the Data Protection Act 1998, which describes how organisations – including YI 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.

Persons in management and supervisory positions must consider how they ensure they and their teams are ensuring that all personal information gathered is protected appropriately. However responsibility also lies with each and every staff member, board member and volunteer in Youth Initiatives.

Our procedures to support the policy are as follows:

Core Principles

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

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

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

This policy helps to protect YI 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 the company uses data relating to them.
- Reputational damage. For instance, the company could suffer it hackers successfully gained access to sensitive data.

Responsibilities

This policy applies to:

- The regional office of YI
- All Youth Community and Area Hubs of YI
- All staff and volunteers of YI
- All contractors, suppliers and other people working on behalf of YI

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photographs of individuals
- Plus any other information relating to individuals

Everyone who works for or with YI has some responsibility for ensuring data is collected, stored and handles appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, the

following people have key areas of responsibility:

- The trustees are ultimately responsible for ensuring that Youth Initiatives meets its legal obligations.
- The data protection officer, Tony Silcock is responsible for:
- Keeping the Trustees 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.

- The Office Manager, Branch Managers and Area Leaders are responsible for:
  - Dealing with requests from individuals to see the data that the YI Hub/ office holds about them (also called 'subject access requests').
  - 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.
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
  - Approving any data protection statements attached to communications such as emails and letters.
  - Working with other staff to ensure marketing initiatives abide by data protection principles.

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 supervisors.
- **YI 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 their Branch Manager/Area Leader or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Officer or the Office manager.

Data stored on paper

When data is **stored on paper**, it should be kept in a secure place where unauthorized people cannot see it. The following 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 or photocopier.
- **Data printouts should be shredded** and disposed of securely when no longer required.

Data stored electronically

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 in **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 is of no value to YI unless the organisation can make use of it. However, it is when personal data is accessed and used that it can 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. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- 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 YI to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort YI should put into

ensuring its accuracy.

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.

• 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. For instance, by confirming a young persons or supporters details when they call.

• YI will make it easy for data subjects to update the information YI holds about them. For instance, via the company website.

• Data should be updated as inaccuracies are discovered. For instance, if a young person or supporter can no longer be reached on their stored telephone number, it should be removed from the database.

• It is the Fundraising Support worlers responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject Access Requests

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

• Ask what information the company holds about them and why.

• Ask how to gain access to it.

• Be informed how to keep it up to date.

• Be informed how the company is meeting its data protection 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 Branch Manager / Area Leader / Office manager. The Branch Manager / Area Leader / Office manager will aim to provide the relevant data within 14 days. The Branch Manager / Area Leader / Office manager will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

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

Under these circumstances, YI will disclose requested data. However, the Branch Manager / Area Leader / Office manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

YI 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, the organisation has a privacy statement, setting out how data relating to individuals is used by the company.

Please see privacy statements in the Appendices section. This privacy statement is available on our website.

Appendix 1: Privacy Statement

Privacy Policy

Youth Initiatives respects the privacy of its supporters, volunteers, employees and the young people who participate in our programmes. Your privacy is important to us. To better protect your privacy we provide this notice explaining our practices for protecting the information and the choices you can make about the way your information is collected and used at our site.

Our principles

We are absolutely committed to protecting your privacy. Our policy can be summarised in one sentence: we will not share your information with others without your consent.

We have established the following principles:

1. We will respect your email privacy. You will only receive email from Youth Initiatives in relation to areas you have expressly signed up for.
2. We will not share any individual user details (including your email address) to any third party without your consent.
3. At Youth Initiatives we value your privacy and will do everything in our power to protect and ensure the confidentiality of any information provided arising from the use of our website.
4. When you submit information via our web site, your information is protected both online and off-line. We do not, however, take responsibility for circumstances beyond our control, which might jeopardise information.
5. Youth Initiatives will not disclose any personal information to a third party without your prior consent. Any information provided in confidence, will be treated with the utmost privacy and will be handled by authorised staff of Youth Initiatives.

The Information We Collect

Youth Initiatives collects personal information of supporters, donors, employees, volunteers, young people and parents; and prayer partners. The information includes: your name, address, e-mail address, telephone number, payment information, your interest in specific types of programmes and/or services an din the case of young people – photos and videos.

How We Use the Information

The reason we collect this information is for the following purpose:

• to send out periodic newsletters, prayer emails etc. From time to time we may also send you additional information about our ministries and/or services in special mailings.

• for gift-aid purposes. For example we may collect bank account information if you are a donor sitting up a direct debit donation.

• Personal information of volunteers is kept in a volunteer record for the purpose of contacting volunteers and scheduling programme hours.

• Personal information of youth may include emergency contact information and is only used to register youth in the centre/ programme, for a specific trip or event, in case of accident, illness or injury during the programme or trip.

• Personal information of youth may also include video footage, photos and/or interviews. This information will be used to help tell the stories of YI, promote ministries and programmes of all YI across Northern Ireland, as well as keep a record of the ongoing work. This may include using photos and/or videos on our website and other YI websites, YI instagram, Facebook and twitter pages; in the creational of promotional material and at events.

• At no time is this information shared with any third party, except in the case of emergency during a programme, trip or event. Personal information of youth is collected on permission forms signed by a parent or guardian for each individual trip or event and are destroyed once the trip or event is concluded.

• Employees of Youth Initiatives may have access to your personal information provided they have a specific need to know in connection with the purposes identified in this privacy policy. Access is permitted only to the extent necessary for such purposes.

• We may disclose personal information in response to legal process (e.g. in response to a court order or subpoena). We also may disclose such information in response to a law enforcement agency's requests. Collection of Information by Third Party Sites.

How We Store the information

Personal information of supporters will be kept either in electronic format or on paper in secure cabinets at the Youth Initiatives office/ hub.

• Employees may keep records of their personal supporters in the local Youth Initiatives office.

• Paper records of donations may also be kept in storage.

• Personal information of volunteers will be kept in the local office to which they donate their time.

• Personal information of youth will be kept in the office which is operating the programme, trip or event that they are attending.

We will honour any request you may make to have access to or review your personal information. If you have questions or concerns about our privacy practices or you do not wish to allow us to use your personal information in any manner described above you may contact us in writing.

Special Note For Parents

While we encourage children to consult with their parents before furnishing personal data, parents should supervise their children's activities both over the internet and online.

Special Note For Young People and Children

Be sure to ask your mom or dad for permission before sending any information about yourself to us (or anyone else) over the Internet or in person.

Contact Details

Attention: Privacy Officer
Youth Initiatives
50 Colin Road
Belfast BT17 OLG

Appendix 2: Internet Privacy Statement

At Youth Initiatives we collect different types of information about our website users for the following reasons:

1. To provide an interactive website where email is used to communicate with the users.
2. To provide a security mechanism whereby we can restrict content to certain groups of users.
3. To help us improve the service we offer.

Who will have access to your information?

You have control over who is able to access specific items of information. By default your information will not be visible to anyone else using the site. You can change these settings from your personal profile page.

What else you should know about internet privacy

Remember to close your browser when you have finished your user session. This is to ensure that others cannot access your personal information and correspondence if you share a computer with someone else or are using a computer in a public place like a library or Internet cafe. You, as an individual, are responsible for the security of your own computer.

Please be aware that whenever you voluntarily disclose personal information over the Internet that this information can be collected and used by others. In short, if you post personal information in publicly accessible online forums, you may receive unsolicited messages from other parties in return. Ultimately, you are solely responsible for maintaining the secrecy of your usernames and passwords and any account information.

Please be careful and responsible whenever you are using the Internet. Our pages may contain links to other websites.. Please be aware that we, Youth Initiatives, are not responsible for the privacy practices of such other sites. We encourage our users to be aware when they leave our site and to read the privacy statements of each and every website that collects personally identifiable information. This privacy statement applies solely to information collected by Youth Initiatives.

Spamming Policy

▪ We maintain a strict "No-Spam" policy which means that we do not intend to sell, rent, or otherwise give your e-mail address to a third-party, without your consent.

▪ In addition, Youth Initiatives will not send you e-mail that you have not agreed to

receive.

▪ We may from time to time send e-mail announcing new Youth Initiatives products and services.

▪ We will at all times include an opt-out message with all e-mail newsletters, in order for you to choose not to receive any further correspondence from us.