NORTHERN IRELAND YOUTH FORUM PRIVACY NOTICE

1. WHO ARE THE NORTHERN IRELAND YOUTH FORUM?

The Northern Ireland Youth Forum (NIYF) is a registered charity in Northern Ireland, with headquarters at 68 Berry Street, Belfast, BT11FJ. Registered Charity: XR36973, NI Charity number: NIC102677.

NIYF is a regional voluntary youth-led voluntary organisation that was established in 1979 by the Department of Education to promote the voice of young people to Government and other decision makers. We work to support young people to raise and discuss issues that are important to them, locally, regionally, nationally and internationality.

Our work is wide ranging and diverse; it is aimed at promoting the voices of young people; building capacity and putting young people at the centre of the policy making process. We are entirely youth led in that the Executive Committee is made up of young people, elected every two years by our membership. Any young person aged between 11 – 25 can become a member of the Youth Forum provided they reside in NI for 70% of their time. Young people living outside of NI can sign up as affiliate members; and youth organisations can join the Youth Forum as organisational members.

2. WHAT IS THIS NOTICE?

This policy sets out NIYF's Northern Ireland's policies and procedures in relation to the General Data Protection Regulations (GDPR). As such, this policy outlines our procedures relating to obtaining, maintaining, processing and destroying personal data.

In order to provide our services , we may need to process personal data from time to time. By personal data we mean information about someone that can be used to identify them. This Personal Data may be about you or other people. This notice explains how we will use the Personal Data we hold.

NIYF has a duty of care to ensure that all our practices are safe, compliant and protect personal data. The charity is committed to safety and our processes are designed to protect those whose personal information we hold.

The Northern Ireland Youth Forum holds personal data about its employees, volunteers, young people, members, stakeholders, partners and other individuals for a variety of documented business proposes. The charity complies with current data protection legislation when obtaining, maintaining and destroying personal data.

As part of the services that we provide, we, from time to time, may transfer Personal Data to other people. We have set out a list of who we might transfer Personal Data to in paragraph 7. This notice only deals with our use of Personal Data. Recipients are not bound by this privacy notice.

We may need to change this privacy notice from time to time. If we do, we will let you know.

All of the defined terms in this notice are explained in paragraph 14 below. If you have any questions about this notice, feel free to send us an email to info@niyf.org

3. WHO DO NIYF HOLD PERSONAL DATA ABOUT?

NIYF hold Personal Data about the following groups of people (**Data Subjects**):

DATA SUBJECTS	DESCRIPTION
Project participants	Any young person aged between 11 – 25 years who currently engages in NIYF programmes
Membership (Youth – individual and affiliate members)	Young people aged between 11 – 25 years who have signed up as members of NIYF as per its constitution
Membership (Organisational)	Individuals who represent organisations who have signed up as members of NIYF as per its constitution
Supporters	That is anyone who has contacted NIYF to find out about what it does or otherwise supported NIYF, other than through Membership; including those who have signed up to receive information via NIYF's e-mail newsletter
Contractual / Project Partnership Data e.g. Staff; funders; contactors	Anyone that provides a service for the Youth Forum including staff. Also including those who we provide services for e.g. funding bodies etc.

4. NIYF IS A DATA CONTROLLER

4.1 NIYF is a Data Controller in respect of the following data – Project participants; Membership (Youth); Membership (Organisational) and Supporters.. This means NIYF makes decisions about what data to collect (in respect of those groups of Data Subjects) and how to use it.

5. WHERE DOES NIYF COLLECT PERSONAL DATA FROM?

Project Participants

Source	Types of Data Collected
Consent Forms	Contact and Identity Data Parental Consent Emergency Contact Details Medical information
Our Website	Traffic Data Usage Data Technical Data
Monitoring Forms	Special Category Data such as an individual's race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, etc.

Membership (Youth)

Source	Types of Data Collected
Consent Forms	Contact and Identity Data Parental Consent Emergency Contact Details Medical information
Membership Sign Up forms	Contact and Identity Data
Our Website	Traffic Data Usage Data Technical Data

Membership (Organisational)

Source	Types of Data Collected
Membership Sign Up forms	Contact and Identity Data
Direct interactions with the Data Subject	Contact and Identity Data Transaction Data Preferences Job Roles and Business Data
Our Website	Traffic Data Usage Data Technical Data
Publically available sources (internet, Companies House)	Contact and Identity Data Job Roles and Business Data

Supporters

Source	Types of Data Collected
Information provided by our Client	Contact and Identity Data

Direct interactions with the Data Subject	Contact and Identity Data Transaction Data Preferences Job Roles and Business Data
Our Website	Traffic Data Usage Data Technical Data
Publically available sources (internet, Companies House)	Contact and Identity Data Job Roles and Business Data

Contractual / Project Partnership Data

Source	**Types of Data Collected**
Contracts; SLAs; MoU's; Working Agreements etc.	Contact and Identity Data Transaction Data Preferences Job Roles and Business Data

It is likely that some of the Personal Data which NIYF collects and stores about Project Participants / Membership (Youth) may include **Special Categories of Personal Data.** Special Categories of Personal Data includes details about an individual's race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about health and genetic and biometric data.

Personal data and special categories of personal data will be captured and stored separately. Special category data will only be stored and / or shared for specific legal purposes, for example as a requirement of a funder.

General

NIYF may also collect, use and share **Aggregated Data** such as statistical or demographic data which we collect from interactions with Project Participants; Our Youth and / or Organisational members etc. Aggregated Data may be obtained from Personal Data but since it cannot be used to identify an individual, it is not Personal Data.

6. HOW NIYF WILL USE THE PERSONAL DATA IT HOLDS AND WHAT ARE THE LAWFUL BASIS FOR DOING SO?

6.1. *Project Participants / Membership (Youth) / Membership (Organisational)*

(i) NIYF hold and process Project Participants / Membership (Youth) / Membership (Organisational) Data as a Controller, which means we must have a 'lawful basis' for doing so.

(ii) In some cases, we may use personal information where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. For example, the Youth Forum has a legitimate interest in providing young people with non formal education, safeguarding and promoting child / youth welfare, facilitating the efficient operation of the organisation.

(iii) Anywhere NIYF are relying on legitimate interest we believe that such processing is necessary for the purposes of our **legitimate interest**, which in this case is to function as a business. We consider such use goes no further than the Data Subject would reasonably expect; is likely to align with the Data Subject's interests (by enabling us to provide a sustainable business model) and is unlikely to be detrimental to the fundamental rights and freedoms of the Data Subject.

(iv) We keep personal information electronically on the Youth Forum's information management systems or manually in indexed, lockable filing systems.

(v) Situations in which we will use personal data, including special category data include:

Teaching & Learning

For example:

- to monitor and report on participant progress
- to provide appropriate pastoral care

Statutory / Funding Body Returns

For example:

- to monitor equal opportunities

Safeguarding & Child Protection

For example:

- to safeguard young people
- referrals to external service providers (with your consent)

Security

For example:

- to comply with health and safety obligations
- to comply with the law regarding data sharing

Business Continuity

For example:

- to assess the quality of our services

Access to Systems

For example:

- to support youth development and progression

Communications

For example:

Sound Financial Management

For example

- to foster links between the orgnisation and the local community, including fundraising events
- provision of incentive payments to project participants

7. WHO NIYF WILL DISCLOSE PERSONAL DATA TO?

We may have to share young people's data with third parties, including third-party service providers and other bodies such as:

- The Department of Education (D.E)
- The Education Authority (E.A)
- Youth Council for Northern Ireland (Y.C.N.I)
- Police Service of Northern Ireland (P.S.N.I) e.g. *Child Protection Issues*
- Health & Social Care Trust Northern Ireland (H.S.C.N.I) e.g. *Child Protection Issue*
- Our funders
- Data Systems such as e.g. Doddle
- Within Closed Groups on Social Media Platforms i.e. group picture on our facebook page

Why we share young people's information

We do not share information about young people with anyone without consent unless the law and our policies allow us to do so. We only permit access to personal data for specified purpose and in accordance with our instructions.

We are required to young people's data with some of our funders including the Department of Education and/or the Education Authority on a statutory basis. This data sharing underpins youth forum funding and related monitoring requirements.

If you have any questions about where your data might be transferred to please send us an email at info@niyf.org

8. CONSENT

Whilst the majority of the personal data provided to the Youth Forum is required for us to comply with our legal obligations, some of that information is provided on a voluntary basis through parental consent (namely, a parent's/carer's/legal guardian's express agreement).

Only young people aged 13 or over are considered capable of giving consent themselves and will not require express agreement from a parent/carer/legal guardian (not relevant in our school).

Where we need consent, the youth forum will provide the person with parental responsibility for a young person or, if aged 13 or over, the young person themselves, with a specific and clear notice which explains the reasons why the data is being collected and how the data will be used. You should be aware if you do not consent to our collection of this type of data, this will not affect the standard of services we deliver to the young person.

If we ask for your consent to use personal information, you can take back this consent at any time by submitting a written request to do so to the school principal. Please be aware that we do not need to obtain parental consent if personal data is to be processed for the purposes of obtaining counselling services for the young person.

9. WHAT SECURITY PROCEDURES NIYF HAVE IN PLACE?

9.1 It is our policy to ensure that all Personal Data held by NIYF is handled correctly and appropriately according to the nature of the information, the risk associated with mishandling the data, including the damage that could be caused to an individual as a result of loss, corruption and/or accidental disclosure of any such data, and in accordance with any applicable legal requirements.

9.2 We will always seek your consent for asking for and keeping your data. We will always explain why we want this and what it will be used for.

9.3 Data will not be kept for longer than is necessary, as per the requirements of data protection legislation. Unrequired data will be destroyed as soon as reasonably practicable in a secure manner. Paper documentation will be shredded and electronic resources will be wiped using appropriate measures.

9.4 As part NIYF's commitment to confidentiality, all data will be secure through the following procedures:

9.4.1 Confidential paper records will be held in a locked filing cabinet, drawer, archive or safe. Access will be restricted and will only be applicable to appropriate individuals.

9.4.2 Confidential paper records will not be left unattended or in clear view in an area with general access.

9.4.3 In cases whereby confidential paper records are required to be transported / taken off NIYF premises the charity expects employees to take every reasonable precaution to protect the data. Employees will take extra care to follow the same procedures for security including taking steps to ensure these records are held in a suitable, lockable, portable storage device; shall never be left unattended in a vehicle and shall be locked away on arrival at destination. The individual taking the data will take full responsibility for the security of the data.

9.4.4 Staff should take similar steps when required to print / photocopy personal data e.g. ensuring no copies are left in or near copier; on desks or in other area that could breach this privacy policy.

9.4.5 Electronic data will be encrypted or held securely in a password-protected area.

9.4.6 Where data is held on a portable or removable storage device, the device will be kept in a secure manner when not in use.

9.4.7 Memory sticks will not be used to hold personal data unless they are password protected and encrypted.

9.4.8 All electronic devices used within the charity will be password protected to protect information in case of theft. Where possible, remote blocking will be enabled in instances of theft.

9.4.9 All members of staff will be provided with their own digital / cloud based storage accounts and will have individual logins and passwords. Passwords will be changed on a regular basis, where appropriate.

9.4.10 Emails or electronic communications which contain sensitive or confidential personal data will be password protected.

9.4.11 Under no circumstances, should staff use personal e-mail accounts for work purposes.

9.4.12 Where the charity uses autofill email addresses, the employee will be expected to take necessary steps to protect the content of the information and NIYF's reputation.

9.4.13 The physical security of NIYF offices is reviewed on a regular basis. If there is an increased risk to security, extra measures will be implemented to secure data.

9.5 NIYF shall adhere to and train staff in relation to the National Cyber Security Centre, Cyber Security Small Charity Guide (see appendix I)

10. Sharing Agreements

10.1. Sharing agreements are contracts between parties which outline the obligations, responsibilities and liabilities in relation to the protection of data. Where appropriate, NIYF will obtain signed sharing agreements with third parties in instances where personal data is shared. This sharing agreement is designed to ensure that third parties have sufficient safeguards in place, concerning the compliance of GDPR.

If your personal data is to be shared with a third party, you will be notified in advance.

11. Staff Training

11.1. Employees will receive information on the requirements of the data protection processes upon commencement of their employment. Training will raise data protection awareness amongst staff and will help them understand their data protection obligations and responsibilities. Employees will be given the tools to ensure that personal data is protected and processed lawfully during the course of their employment. Should training updates or refreshers be required, this will be carried out without delay. Employees are required to complete all assigned data protection training as requested; all training undergone will be signed off by the employees and documented as appropriate.

12. TRANSFERRING DATA OUTSIDE THE EU

12.1. We will not transfer the personal information we collect about you to any country outside the EU without telling you in advance that we intend to do so and what steps we have taken to ensure adequate protection for your personal information in those circumstances.

13. HOW LONG NIYF STORES PERSONAL DATA?

13.1. Our retention policies for Project Participants / Membership (Youth) / Membership (Organisational) Data are as follows:

(a) Project Participants – NIYF may store data up to 2 years after the project is finished;
(b) Membership (Youth) – NIYF may store data up until your 26th Birthday;
(c) Membership (Organisational) – NIYF may store data indefinitely or as long as organisations want to remain members of the Youth forum;
(d) Supporters - NIYF may store data indefinitely or as long as organisations want to continue receiving information about the work of the Youth forum;

13.2 Our retention policies for Contractual / Project Partnership Data are as follows:

(a) NIYF may store data related to financial transactions for up to 7 years to ensure that we have sufficient records from an accounting and tax perspective;

(b) We may archive data relating to negotiations, contracts agreed, payments made, disputes raised and your use of our software for up 7 years to protect ourselves in the event of disputes arising between NIYF and other parties;

(c) We may retain data which is held for marketing purposes for up to 3 years from the date of termination of our contract with you (unless the relevant Data Subject requests erasure of their data prior to that date);

(d) We may store aggregate data without limitation (on the basis that no individual can be identified from the data).

14. THE RIGHTS OF A DATA SUBJECT IN RELATION TO THE PERSONAL DATA WE COLLECT AND HOLD?

14.1 Data Subjects have the following rights in respect of Personal Data relating to them which can be enforced against whoever is the **Controller**.

(a) Right to be informed: the right to be informed about what Personal Data the Controller collects and stores about you and how it is used.

(b) Right of access: the right to request a copy of the Personal Data held, as well as confirmation of:

(i) the purposes of the processing;
(ii) the categories of personal data concerned;
(iii) the recipients to whom the personal data has/will be disclosed;
(iv) for how long it will be stored; and
(v) if data wasn't collected directly from the Data Subject, information about the source.

(c) **Right of rectification:** the right to require the Controller to correct any Personal Data held about the Data Subject which is inaccurate or incomplete.

(d) **Right to be forgotten:** in certain circumstances, the right to have the Personal Data held about the Data Subject erased from the Controller's records.

(e) **Right to restriction of processing**: the right to request the Controller to restrict the processing carried out in respect of Personal Data relating to the Data Subject. You might want to do this, for instance, if you think the data held by the Controller is inaccurate and you would like to restrict processing the data has been reviewed and updated if necessary.

(f) **Right of portability:** the right to have the Personal Data held by the Controller about the Data Subject transferred to another organisation, to the extent it was provided in a structured, commonly used and machine-readable format.

(g) **Right to object to direct marketing:** the right to object where processing is carried out for direct marketing purposes (including profiling in connection with that purpose).

(h) **Right to object to automated processing:** the right not to be subject to a decision based solely on automated processing (including profiling) which produces legal effects (or other similar significant effects) on the Data Subject.

If you want to avail of any of these rights, you should contact us immediately at info@niyf.org. If we are not the Controller, we will need to transfer your request to the Controller – but we will only do so with your consent. If you do contact us with a request, we will also need evidence that you are who you say you are to ensure compliance with data protection legislation.

15. WHAT HAPPENS IF I NO LONGER WANT YOU TO PROCESS PERSONAL DATA ABOUT ME?

15.1 If we are holding Personal Data about you as a Controller, we will comply with your request unless we have reasons for lawfully retaining data about you.

15.2 If we are holding Personal Data about you and using that data for marketing purposes or for any other activities based on your consent, you may notify us at any time that you no longer want us to process Personal Data about you for particular purposes or for any purposes whatsoever and we will stop processing your Personal Data for that purpose. This will not affect your ability to receive our Services.

16. WHO DO I COMPLAIN TO IF I'M NOT HAPPY WITH HOW YOU PROCESS PERSONAL DATA ABOUT ME?

16.1 If you have any questions or concerns about how we are using Personal Data about you, please contact our Data Protection Officer immediately at our registered address (see paragraph 1.1 above).

16.2 If you wish to make a complaint about how we have handled Personal Data about you, you may lodge a complaint with the Information Commissioner's Office by following this link: https://ico.org.uk/concerns/

17. WHAT DO ALL OF THE DEFINED TERMS IN THIS PRIVACY NOTICE MEAN?

17.1 Throughout this notice you'll see a lot of defined terms (which you can recognise because they're capitalised). Where possible, we've tried to define them as we go, but we thought it might be useful to have a glossary at the end for you. Anywhere in this notice you see the following terms, they'll have the following meanings:

Controller is a legal term set out in the General Data Protection Regulation (**GDPR**), it means the party responsible for deciding what Personal Data to collect and how to use it;

Data Subject means the individual who can be identified from the Personal Data;

Personal Data means data which can be used to identify a living individual. This could be a name and address or it could be a number of details which when taken together make it possible to work out who the information is about. It also includes information about the identifiable individual;

Processor is another legal term set out in the GDPR, it means the party who has agreed to process Personal Data on behalf of the Controller; and

Special Categories of Personal Data means details about an individual's race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about health and genetic and biometric data.

Last updated: 24th May 2018

APPENDIX I

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked, remotely wiped** or **remotely locked.**

Keep your **devices** (and all **installed apps**) **up to date,** using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs.**

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges.** This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar,** or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc