



Global Youth Network for Quality and Excellence – GYNQE

(Privacy Policy and Data Protection Policy)

2026

Privacy Policy and Data Protection Policy

Global Youth Network for Quality and Excellence

Effective Date: 12 August 2026

Version No.: 1.0

Introduction

This Policy explains how the personal data of members, visitors and participants of the Global Youth Network for Quality and Excellence are collected, used, retained, shared and protected; the rights available to data subjects; and the mechanisms for communication and for submitting relevant requests or complaints.

Data protection and privacy are among the fundamental principles governing Network membership, alongside adherence to its Charter and Code of Conduct, respect for diversity and intellectual property, and responsible participation.

This Policy is guided by the principles of fair processing, purpose limitation, necessity and proportionality, data accuracy, storage limitation, confidentiality, security, transparency and accountability. These principles are consistent with UNESCO's Personal Data Protection and Privacy Framework.

First: Scope of Application of the Policy

This Policy applies to data collected or processed through:

- The Network website and online portal.
- The membership platform and personal profiles.
- The Youth Club and digital communities.
- Applications associated with the Network.
- Registration and joining forms.
- Surveys, studies and focus groups.
- In-person and virtual events and meetings.
- Training and academic courses.

- Innovation and foresight laboratories.
- The ambassadors and coordinators programme.
- Working groups and the Youth Council.
- Newsletters and notifications.
- Official social media platforms.
- Technical support, complaints and reporting systems.
- Certificates and digital cards.
- Any service or activity conducted under the Network's name.

It also applies to:

- Youth members.
- Founding members.
- Ambassadors and coordinators.
- Members of the Youth Council.
- Applicants for programmes and opportunities.
- Experts, mentors and trainers.
- Volunteers.
- Institutional partners.
- Website visitors.
- Survey and event participants.
- Representatives of cooperating entities.
- Parents or guardians, where needed.

Second: Entity Responsible for Data

The Network's Technical Secretariat at the UNESCO Regional Center for Quality and Excellence in Education oversees the management of data associated with the Network, including:

- Determining the purposes for collecting data.
- Approving forms and systems.
- Managing access permissions.
- Reviewing service providers.
- Responding to data-subject requests.
- Managing incidents and reports.
- Supervising deletion and retention.
- Documenting processing operations.
- Verifying compliance with this Policy.

Third: Terms and Definitions

For the purposes of this Policy, the following terms have the meanings set out opposite them:

Personal Data

Any information relating to an identified or identifiable natural person, directly or indirectly, such as a name, email address, membership number, photograph or device identifiers.

Sensitive Data

Data whose disclosure or misuse may result in greater harm, such as health data, disability data, biometric data, precise location data, or certain social, crisis-related or protection-related information.

Data Subject

The person to whom the personal data relate.

Data Processing

Any operation performed on data, such as collecting, recording, organizing, retaining, modifying, analysing, sharing, transferring or deleting it.

Data Controller

The entity that determines the purposes and means of processing personal data.

Data Processor

An external entity that processes data on behalf of the Network, such as a hosting provider, email provider or event platform.

Consent

A clear, specific and informed affirmation by the data subject permitting the processing of their data for a particular purpose.

Minor

Any person who has not reached the legally prescribed age for independently consenting to the processing of their data under applicable law.

Anonymisation or De-identification

The removal or alteration of information that permits data to be linked to a specific person.

Fourth: Principles Governing Data Processing

The Network is committed to the following principles:

1. Fairness and Lawfulness

Data are processed fairly and for lawful purposes connected with the Network's mission and activities.

2. Transparency

Members are clearly informed about:

- The data that are collected.
- The purposes for which they are used.
- The entities that may access them.
- The retention period.
- Their rights and how to exercise them.

3. Purpose Limitation

Data are collected only for specific and clear purposes and are not subsequently used in a manner incompatible with those purposes.

4. Data Minimisation

The Network collects only the data that are necessary and does not request additional information merely because it may be useful in the future.

5. Accuracy

The Network takes reasonable measures to ensure that data are accurate and up to date and to correct inaccurate data.

6. Storage Limitation

The Network does not retain data longer than necessary to achieve the purpose or fulfil legal and contractual requirements.

7. Security and Confidentiality

The Network applies administrative, technical and organizational measures to protect data from loss, damage or unauthorized access.

8. Accountability

The Network documents data-processing operations, assigns responsibilities, monitors compliance and reviews procedures periodically.

9. Privacy by Design

Privacy is taken into account from the design stage of the platform, forms and services, not only after they are put into operation.

10. Protection of the Interests of Youth and Minors

Priority is given to the safety and best interests of youth, and additional safeguards are applied when processing minors' data. Recent UNICEF guidance stresses the importance of integrating privacy, digital safety and child protection from the design stage of digital infrastructure and services.

Fifth: Types of Data the Network May Collect

1. Basic Identification Data

- First and last name.
- Name in English.
- Username.
- Date of birth or age group.
- Gender, where needed and optionally wherever possible.
- Nationality.
- Country and city.
- Profile photograph, if the member chooses to upload it.
- Membership number.

2. Contact Data

- Email address.
- Telephone number.
- Preferred language.
- Correspondence address, where needed.
- Communication and notification preferences.

3. Educational and Professional Data

- University or institution.
- Field of specialization.
- Educational level.
- Job title.
- Employer.
- Experience.
- Skills.
- Professional links.
- Curriculum vitae when applying for a specific opportunity.

4. Interest and Participation Data

- Areas of interest.
- Working groups.
- Activities for which the member is registered.
- Attendance and participation.
- Completed courses.
- Badges and certificates.
- Ideas and initiatives submitted.
- Contributions to discussions.
- Mentoring and volunteering requests.

5. Survey and Research Data

- Closed and open-ended responses.
- Youth opinions and aspirations.
- Priorities and challenges.
- Demographic data required for analysis.

- Audio or video recordings, where separate consent has been obtained.
- Outputs from focus groups and interviews.

6. Technical Data

- Internet Protocol address.
- Device and browser type.
- Operating system.
- Language.
- Login times.
- Pages used.
- Activity log.
- Session identifiers.
- Failure and performance data.
- Cookies.

Many digital platforms, including UNESCO's platform, collect technical activity data such as Internet address, device type and browsing behaviour for operational and analytical purposes; users must be clearly informed of this.

7. Support and Complaint Data

- The content of the enquiry or report.
- Related correspondence.
- Supporting evidence or attached files.
- Actions taken.
- Processing outcome.
- Confidentiality preferences.

8. Visual and Media Data

- Photographs.
- Video and audio recordings.
- Interviews.
- Success stories.
- Quotations.
- Media materials.

These materials are used only pursuant to clear notice and consent, particularly where minors are involved.

9. Accessibility and Accommodation Data

Limited information may be collected regarding:

- Disability.
- Translation needs.
- Digital accommodations.
- Attendance requirements.

Providing this information is optional, and it is used only to provide appropriate accommodations and protection.

Sixth: Data That Should Not Be Requested Except Where Necessary

The Network does not normally request:

- National identity number.
- Passport number.
- Banking data.
- Precise geographical location.
- Detailed health data.
- Biometric data.

- Political background.
- Passwords for other services.
- Contact details of other persons.

If collecting any of these becomes necessary for a legitimate and specified purpose, a separate notice shall be provided explaining the reason, duration and safeguards.

Seventh: Sources of Data Collection

The Network collects data through:

- Data provided directly by the member.
- Registration forms.
- The personal profile.
- Applications to participate in programmes.
- Surveys.
- Support messages.
- Participation on the platform.
- Attendance at events.
- Nomination by a partner entity, after an appropriate basis and consent have been established where required.
- Technical data collected automatically.
- Public professional sources to which the member personally provides a link.

The Network does not rely on purchasing youth databases or covertly collecting data from the Internet.

Eighth: Purposes of Using Data

Data are used for the following purposes:

1. Membership Administration

- Creating the account.
- Verifying the email address.
- Reviewing the application.
- Issuing a membership number.
- Issuing a certificate.
- Managing membership status.
- Communicating regarding the account.

2. Personalising the Member Experience

- Suggesting programmes and pathways.
- Connecting the member to interest groups.
- Sending relevant opportunities.
- Providing appropriate language and accommodations.

3. Managing Activities and Programmes

- Recording attendance.
- Organizing meetings.
- Managing training.
- Forming working teams.
- Managing laboratories and initiatives.
- Selecting participants in accordance with published criteria.

4. Operating the Youth Club

- Enabling introduction and communication.
- Managing groups and posts.
- Supervising content.

- Applying the Code of Conduct.
- Investigating reports.

5. Research and Surveys

- Capturing youth voices.
- Analysing priorities.
- Preparing reports.
- Foresighting trends.
- Developing programmes and policies.

Results should preferably be published in aggregated or anonymised form that does not permit the identification of individuals.

6. Measuring Performance and Impact

- Measuring participation.
- Following up active membership.
- Evaluating programmes.
- Developing services.
- Preparing Network indicators.

7. Communication and Media

- Sending operational messages.
- Sending invitations and reminders.
- Issuing newsletters.
- Publishing success stories with their owners' consent.

8. Protection and Security

- Preventing misuse.
- Detecting fake accounts.
- Investigating violations.
- Protecting members and the platform.

- Addressing cybersecurity incidents.

9. Fulfilling Legal or Contractual Obligations

- Maintaining consent records.
- Managing partnerships.
- Responding to valid legal requests.
- Documenting programmes and funding where needed.

Ninth: Basis for Processing

Depending on the type of data, the purpose and the applicable law, processing may be based on:

- The consent of the data subject.
- Performance of a membership or service request.
- Fulfilment of contractual obligations.
- A legitimate interest connected with operating and protecting the Network.
- A legal obligation.
- Protection of a person's vital interests.
- The best interests of the young person or minor, within the prescribed safeguards.
- The Center's mandate and institutional competencies.

Separate and clear consent must be obtained in cases such as:

- Publishing photographs and stories.
- Subscribing to marketing messages.
- Video recordings.
- Using data in new, unforeseen research.
- Sharing the personal profile with external entities.
- Processing optional sensitive data.

Tenth: Consent and Its Management

Consent must be:

- Clear.
- Purpose-specific.
- Informed.
- Separate from the general terms where needed.
- Capable of being evidenced.
- Capable of being withdrawn.

Consent does not affect an essential service if the data subject to consent are not necessary to provide that service.

The member may:

- Change communication preferences.
- Unsubscribe from newsletters.
- Withdraw consent to publish a photograph.
- Withdraw consent to optional processing.
- Request the removal of published personal content.

Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal.

Eleventh: Data of Minors

If the Network permits the membership or participation of persons below the legally prescribed age, the following measures shall apply:

1. Clearly determining the minimum age.
2. Reasonably verifying age.
3. Obtaining parental or guardian consent where required by law.
4. Providing a simplified, age-appropriate privacy notice.
5. Collecting the minimum possible amount of data.
6. Disabling the display of location and direct contact by default.

7. Restricting private messages.
8. Not publishing the full name or photograph without specific consents.
9. Preventing exploitative advertising or recommendations.
10. Providing an easy reporting and protection mechanism.
11. Reviewing service providers from a child-protection perspective.
12. Taking the minor's best interests into account in all decisions.
13. Not using minors' data to build commercial or marketing profiles.
14. Not publishing their research contributions in a manner that permits their identification without justification and consent.

UNICEF notes that children face particular risks relating to data misuse, unsafe communication and deceptive digital designs, which require high-privacy settings and age-appropriate protection.

Twelfth: Display of the Member Profile within the Network

Profile data are private by default, and only the minimum information selected by the member is visible to other members, such as:

- First name.
- Country.
- Professional field.
- Interests.
- Brief biography.
- Badges.
- Photograph, if the member chooses to display it.

The following are not displayed by default:

- Telephone number.
- Email address.
- Full date of birth.
- Residential address.

- Precise location.
- Documents.
- Complaint data.
- Individual survey responses.

The member can control:

- Profile visibility.
- Receiving contact requests.
- Photograph visibility.
- Appearance on the member map.
- Displaying the institution or university.
- Receiving messages.

Thirteenth: Member Map and Public Statistics

The Network may display:

- Number of members.
- Number of countries.
- Regional distribution.
- Areas of greatest interest.
- Aggregated participation statistics.

The public map does not display:

- Member names.
- Precise locations.
- Contact addresses.
- Information that permits the identification of a member in a country with very few members.

Fourteenth: Sharing Data with Other Parties

The Network may share limited data with:

- Cloud-hosting providers.
- Email providers.
- Event and meeting platforms.
- Learning systems.
- Analytics providers.
- Platform developers and support providers.
- Certificate-issuing entities.
- Programme partners where necessary.
- Competent legal authorities upon a valid request.

Sharing shall occur only in accordance with the principles of:

- Necessity.
- Data minimisation.
- Purpose limitation.
- Confidentiality.
- Security.
- The existence of an appropriate agreement or contractual commitment.
- Prohibiting the use of data for unauthorized independent purposes.

UNESCO's principles affirm that transfer of data to a third party should be conditional upon the recipient's provision of appropriate data protection.

Fifteenth: What the Network Does Not Do with Data

The Network does not:

- Sell member data.
- Rent contact lists.
- Share data for unauthorized commercial advertising purposes.
- Publish personal data publicly without consent.
- Use youth data for political propaganda.
- Create hidden sensitive profiles about members.
- Use photographs in unforeseen new campaigns without appropriate permission.
- Share individual survey responses with employers or universities.
- Make fully automated consequential decisions without appropriate human review.

Sixteenth: Cross-Border Data Transfers

Given the Network's global nature, data may be stored or processed in a country different from the member's country.

Before transfer, the following measures shall be considered:

- Identifying the storage location.
- Assessing the level of data protection provided by the recipient.
- Signing data-processing and data-transfer agreements.
- Using encryption.
- Defining access permissions.
- Notifying data subjects where needed.
- Obtaining required consents or authorizations.
- Complying with transfer restrictions set out in applicable laws.

If members from the European Union participate or their data are processed within its scope, the requirements of the General Data Protection Regulation may apply, including transparency, data-subject rights and international-transfer safeguards.

Seventeenth: Service Providers

Before contracting with any technical provider, the Network verifies:

- The level of cybersecurity.
- The location of data centres.
- Privacy policies.
- Backup procedures.
- Incident management.
- The ability to delete and restore data.
- Prohibition of using data to train models or for independent purposes without authorization.
- Subcontracting.
- The retention period.
- Commitment to protecting minors.
- The provider's ability to support data-subject rights.

A data-processing agreement must be included that specifies:

- The subject matter of processing.
- Its duration.
- The type of data.
- The purposes of processing.
- Confidentiality obligations.
- Security measures.
- Incident reporting.
- The return or deletion of data upon termination of the contract.
- The right to audit or verify.

Eighteenth: Cookies and Similar Technologies

The platform may use:

- Files necessary for logging in.
- Files for saving language and preferences.
- Files for measuring performance.
- Analytics tools.
- Files for securing sessions.

The following must be ensured:

- A clear cookie notice is displayed.
- Non-essential files are not activated before consent, where required.
- The option to accept, reject or customize them is available.
- Analytics are not linked to identity except where necessary.
- The duration of each file is specified.
- A means is provided to modify preferences later.

UNESCO's digital notices explain the use of cookies and browsing data and enable the user to control them.

Nineteenth: Marketing and Electronic Messages

Messages are divided into:

Operational messages

Such as:

- Account confirmation.
- Membership acceptance message.
- Password recovery.
- Security notices.
- An important terms update.
- Reminders of an activity for which the member is registered.

They may be sent because they are necessary to operate the service.

Optional messages

Such as:

- Newsletters.
- General opportunities.
- Awareness campaigns.
- Partner news.

They are sent only in accordance with appropriate consent, with an easy unsubscribe option.

Twentieth: Photographs, Recordings and Stories

Before publishing a photograph, recording or personal story, the following must be explained:

- The purpose.
- Publication channels.
- Geographical scope.
- Duration of use.

- The possibility of withdrawal.
- Whether the content will be published in the person's name.

Separate consent forms are used in cases of:

- Individual photographs.
- Interviews.
- Success stories.
- Promotional materials.
- Participation of minors.

Giving media consent is not required to obtain basic membership in the Network.

Twenty-First: Research and Surveys

When conducting research or a survey, the Network is committed to the following:

- Providing clear information about the purpose.
- Making participation voluntary.
- Clarifying the duration of the survey.
- Specifying whether the response is anonymous.
- Separating identity from responses wherever possible.
- Restricting access to raw data.
- Publishing results in aggregated form.
- Not using responses to evaluate the individual without informing them.
- Obtaining ethical review when the nature of the study requires it.
- Applying additional procedures when minors or crisis-affected groups participate.
- Specifying the retention period for research data.

Twenty-Second: Automated Decisions and Artificial Intelligence

The Network may use automated systems for limited tasks, such as:

- Suggesting programmes.
- Classifying interests.
- Detecting duplicate registrations.
- Summarising aggregated results.
- Supporting content search.

A decision that substantially affects a member's rights, such as rejection, sanction or final selection, may not be based solely on automated processing without:

- Human oversight.
- Published criteria.
- The possibility of review.
- Correction of errors.
- Objection where appropriate.

Personal or confidential data may not be entered into unapproved public artificial-intelligence tools.

Twenty-Third: Information Security

Depending on the level of risk, the Network applies measures such as:

- Encryption of communications.
- Encryption of sensitive data.
- Multi-factor authentication for administrative accounts.
- Separation of permissions.
- The principle of least privilege.
- Backups.
- Periodic testing.

- Software updates.
- Vulnerability management.
- Audit logs.
- Monitoring login attempts.
- Protection of forms against automated use.
- Review of employee and contractor accounts.
- Revoking access upon the end of an assignment.
- Training the team on privacy.
- An incident-response plan.
- Testing data recovery.

UNESCO's principles emphasize the need to adopt appropriate organizational, administrative, physical and technical safeguards against unauthorized access, loss or damage.

Twenty-Fourth: Control of Access to Data

Permissions are granted according to the role and actual need, such as:

- System administrator.
- Membership manager.
- Programme officer.
- Privacy officer.
- Support officer.
- Data analyst.
- Youth Club supervisor.

Not all officials are granted comprehensive access.

The following must be ensured:

- Documenting the granting of permissions.

- Reviewing them periodically.
- Revoking them immediately when the need ends.
- Prohibiting shared accounts.
- Logging sensitive operations.
- Separating complaint data from general membership data.

Twenty-Fifth: Data Retention Period

The Network adopts an approved retention schedule, which may be as follows after legal review:

Data Type	Proposed Retention Period
Incomplete application	6 months
Rejected application	One year
Active member data	For the duration of membership
Withdrawn member data	30–90 days for implementation, then deletion or anonymisation
Consent records	For the processing period and an additional legal period
Attendance records and certificates	5 years or as required institutionally
General support tickets	Two years
Reports and investigations	According to their severity and legal requirements
Technical analytics data	12 months or less
Anonymised surveys	May be retained for research purposes
Video recordings	According to the notice, consent and purpose
Backups	According to a specified deletion cycle

Final periods must not be adopted until they are aligned with laws, contracts and institutional needs.

Twenty-Sixth: Data Deletion and Destruction

Upon expiry of the purpose or retention period:

- Data are deleted from active systems.
- They are deleted or replaced in backups in accordance with the technical cycle.
- Paper files are securely destroyed.

- Access permissions are revoked.
- Statistical data may be anonymised instead of deleted.
- Deletion implementation is documented in sensitive cases.

Account deletion does not always mean deletion of:

- Records that must be retained by law.
- Anonymised data.
- Content in which others participated if it cannot be separated, with the member's identity removed as far as possible.
- Investigation records that require retention.

Twenty-Seventh: Rights of Data Subjects

In accordance with applicable law and the nature of processing, the data subject may request:

1. To know the data that the Network processes about them.
2. To obtain a copy of them.
3. To correct inaccurate data.
4. To complete incomplete data.
5. To delete data.
6. To restrict processing.
7. To object to certain types of processing.
8. To withdraw consent.
9. To transfer data in an appropriate format, where applicable.
10. To unsubscribe from messages.
11. To object to an automated decision.
12. To know the entities with whom data have been shared.
13. To submit a complaint.
14. To request review of a decision concerning their data.

Providing access, correction and deletion, insofar as this does not impair the legitimate purpose of processing, is consistent with the principle of transparency in UNESCO's framework.

Twenty-Eighth: How to Submit a Data-Related Request

The request is submitted through:

- The electronic privacy form.
- The official email of the privacy officer.
- Personal profile settings, if the feature is available.

The data subject is asked to:

- Specify the type of request.
- Provide sufficient information to verify identity.
- Clarify the relevant data or service.
- Specify how the response is to be received.

The Network shall:

1. Confirm receipt of the request.
2. Verify identity.
3. Assess the request.
4. Search the relevant systems.
5. Fulfil the request or state the reason why it cannot be fulfilled.
6. Document the action.
7. Respond within the period specified by law or institutionally.

No more identification documents than necessary for verification are requested.

Twenty-Ninth: Security Incidents and Data Breaches

A security incident is any event that results in:

- Loss of data.
- Unauthorized access.
- Accidental disclosure.
- Unlawful modification.
- Destruction of data.
- System disruption.
- Sending data to the wrong person.
- Theft of a device containing data.

Response Procedures

1. Containing the incident.
2. Protecting evidence.
3. Assessing the type of data and number of affected persons.
4. Determining the level of risk.
5. Informing the responsible officials.
6. Notifying the competent authorities where required.
7. Notifying affected persons if the risk is high or where required by law.
8. Remedying the cause.
9. Documenting the incident.
10. Reviewing controls to prevent recurrence.

Thirtieth: Privacy-Related Complaints and Reports

A member may submit a complaint if they believe that:

- Their data have been used without permission.
- Their information has been published publicly.
- Their request has not been processed.

- Access permissions have been misused.
- A partner entity has used data for a different purpose.
- A data breach or disclosure has occurred.
- Their consent or preferences have not been respected.

The complaint is handled confidentially, and its submitter is protected from retaliation.

Thirty-First: External Links and Platforms

The platform may contain links to:

- Zoom.
- Social media platforms.
- Learning platforms.
- Partner websites.
- External forms or tools.

The privacy policies of those entities apply to their use. UNESCO explains in its notice that links to external websites are not automatically subject to its privacy notice; users should therefore be directed to read the policies of each external service.

The Network is committed to selecting services carefully, but it does not fully control the practices of external websites.

Thirty-Second: Member Responsibilities

The member is committed to the following:

- Protecting their password.
- Not sharing their account.
- Updating their data.
- Not publishing sensitive information.
- Respecting the privacy of others.
- Not downloading or reusing member data.

- Reporting suspicious accounts or messages.
- Using privacy settings.
- Exercising caution when communicating outside the platform.
- Not sending personal documents through unapproved channels.

Thirty-Third: Training and Awareness

The Network is committed to providing:

- Training for the membership team.
- Training for Youth Club supervisors.
- Awareness for ambassadors and coordinators.
- Simplified guidance for members.
- Additional guidance for handling minors' data.
- Periodic training on incidents and breaches.
- Awareness materials on phishing and fraud.
- An annual review of policies and procedures.

Thirty-Fourth: Privacy Risk Assessment

An impact or risk assessment is conducted before:

- Launching a new technical system.
- Collecting sensitive data.
- Processing minors' data on a large scale.
- Using artificial intelligence.
- Implementing advanced monitoring or analytics.
- Sharing data with a new partner.
- Transferring data to another country.
- Linking multiple databases.
- Launching a public map or membership directory.

The assessment includes:

- The purpose.
- Necessity.
- Risks.
- Affected categories.
- Preventive measures.
- Less intrusive alternatives.
- The approval or modification decision.

Thirty-Fifth: Policy Updates

This Policy is reviewed periodically and when:

- The platform changes.
- A new programme is added.
- A service provider changes.
- Laws are amended.
- A material incident occurs.
- New data processing begins.
- A mobile application is added.

When a material change is made:

- The new version is published.
- The effective date is stated.
- Members are notified.
- New consent is requested where necessary.
- Previous versions are retained.

Thirty-Sixth: Acknowledgment and Consent

When creating an account or submitting a membership application, the user acknowledges that they:

- Have read the Privacy Policy.
- Understand the types of data and the purposes for which they are used.
- Have consented to the processing necessary to provide membership and services.
- Understand that optional consents are independent.
- Know how to exercise their rights.
- Are responsible for the accuracy of the data they provide.

Consent Wording in the Registration Form

I acknowledge that I have read the Privacy and Data Protection Policy of the Global Youth Network for Quality and Excellence and understand how my data are collected, used, retained and protected. I consent to the processing of data necessary to establish my membership and provide Network services in accordance with this Policy.

Optional Messages Consent

I agree to receive news, opportunities and non-operational newsletters and understand that I may unsubscribe at any time.

Photographs and Media Consent

I voluntarily agree to the use of my photographs, recordings or story in the media materials specified in the separate consent form.

Thirty-Seventh: Short Wording for Publication in the Registration Form

The Network collects data necessary to establish membership, manage programmes, communicate and measure impact. It is committed to using them only for the stated purposes, protecting them with appropriate measures and not selling or publishing them without consent. The member may request access to, amendment or deletion of their data in accordance with approved safeguards. The Network also applies additional protection to the data of minors and groups most exposed to risk.

Thirty-Eighth: Approved Institutional Wording

The Global Youth Network for Quality and Excellence is committed to protecting personal data and privacy by processing data fairly, transparently and for specified purposes; collecting the minimum necessary data; maintaining their accuracy, confidentiality and security; and not retaining them longer than necessary. It also enables data subjects to exercise their rights, applies special safeguards to protect minors, regulates data sharing and transfers, and adopts appropriate technical and administrative measures and clear procedures to respond to incidents and complaints.