Youth for Christ Data Protection Policy

This Data Protection Policy referred to herein as our "Privacy Standard" forms part of the information security framework and should be read in conjunction with the Information Security Policy and other related policies.

1. Introduction

Youth for Christ recognises and affirms the rights of every individual in respect of their Personal Data. We understand that the correct and lawful treatment of this Personal Data will maintain confidence in the Youth for Christ movement and will support successful operations. The General Data Protection Regulation (GDPR) also requires that we are able to demonstrate compliance – that is, we need to be able to show that we are meeting all the requirements of GDPR. The correct and lawful treatment of Personal Data by Youth for Christ will maintain confidence in our organisation. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.
We are therefore setting out in this Privacy Standard clear policy, responsibilities and codes of practice which you must read, understand and comply with when Processing Personal Data on our behalf. It sets out what we expect from you in order for Youth for Christ to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Any breach of the Privacy Standard may result in disciplinary action.

This Privacy Standard should be read in conjunction with the **Information Security Policy** and other associated policies. It is an internal document and cannot be shared with third parties without prior authorisation from the DPO. The Privacy Standard is designed to ensure that Youth for Christ:

a. Protects the rights of all contacts, staff and volunteers.
b. Complies with GDPR and follows good practice.
c. Is open about what Personal Data it stores and Processes and how this is done.
d. Protects itself from the risk of data breach.

2. Why this Privacy Standard exists

This Privacy Standard describes how this Personal Data is to be collected, stored, Processed, accessed and disposed of to comply with relevant legislation, in particular the GDPR, Privacy of Electronic Communications Regulation (PECR) and the Fundraising Regulator's Code of Fundraising Practice (CFP).

3. Privacy Standard scope

This Privacy Standard:

a. Covers all Personal Data held or Processed by Youth for Christ, however it is stored - whether in digital media, on paper or any other media.
b. Does not form part of any employee's contract of employment and may be amended at any time.
c. Applies to the national organisation of British Youth for Christ and is also a core policy for chartered ministries of Youth for Christ in Britain to follow.

d. Is an internal document and cannot be shared with third parties without prior authorisation of the Data Protection Officer (DPO).

4. Data protection terms

Annex A gives a full explanation of the data protection terms used in this Privacy Standard.

5. Data protection principles

Anyone Processing Personal Data must comply with the fair and lawful principles set out in the GDPR. These require that our handling of Personal Data must be:

a. Processed lawfully, fairly and transparently – there must a legal basis for Processing Personal Data (which includes obtaining, holding, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it). Processing must be done lawfully, fairly and in a manner open and transparent to the individuals concerned – this includes any transfer of the data to third parties.
b. Collected only for specified, explicit, legitimate and prescribed charitable purposes – these include fundraising, personnel/employee/volunteer administration, charity and voluntary organisational objectives, public relations and external affairs, purchase/supplier information, and customer/client information.
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
d. Accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purpose for which it is Processed, is erased or rectified without delay.
e. Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed; Personal Data may be stored for longer periods insofar as the Personal Data will be Processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
f. Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.
g. Protected by design – all procedures and processes need to be designed with data protection in mind. We need to build compliance with legal requirements and good practice into the design stage of projects and changes. Personal data should not be transferred to another country without appropriate safeguards being in place. Youth for Christ is responsible for and must be able to demonstrate compliance with the data protection principles listed above.

6. Legal rights of Data Subjects

GDPR makes clear that the people about whom we hold and Process Personal Data (Data Subjects) have clear legal rights as set out in the next section. As well as complying with the requirements for security and transparency, Youth for Christ has to have a legal basis for Processing Personal Data. The GDPR allows Processing for specific purposes, some of which are set out below:

a. The Data Subject has given his or her consent.
b. The Processing is necessary for the performance of a contract with the Data Subject.
c. For compliance with a legal obligation to which Youth for Christ is subject.
d. To protect the vital interests of the Data Subject.
e. The Processing is necessary for a task carried out in the public interest or in the exercise of official authority.

f. For the legitimate interests pursued by the Youth for Christ or a third party (except where these interests are overridden by the interests or fundamental rights and freedoms of the Data Subject).

A Data Subject consents to the Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, explicit consent is usually required for Processing Sensitive Personal Data, and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue to the Data Subject a separate Privacy Notice to capture explicit consent.

You will need to evidence consent captured and keep records of all Consents so that Youth for Christ can demonstrate compliance with consent requirements.

When Sensitive Personal Data is being Processed, additional conditions must be met.
Clear legal grounds are required to Process Sensitive Personal Data and any consent must explicitly cover the sensitive data being Processed.

7. Notifying Data Subjects

If we collect Personal Data directly from Data Subjects, we will inform them about the purpose or purposes for which we intend to Process their Personal Data and the legal basis for Processing. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

We will also explain their rights, including:

a. The right to be informed.
b. The right of access.
c. The right to rectification.
d. The right to erasure.
e. The right to restrict Processing.
f. The right to data portability.
g. The right to object.
h. The right not to be subject to automated decision-making including profiling.

Wherever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with all the information required by the GDPR including the fact that we are the Data Controller with regard to that data, as well as how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

If we receive Personal Data about a Data Subject indirectly (in other words from other sources), we will provide the Data Subject with the information required by the GDPR as soon

as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

8. Adequate, relevant and non-excessive Processing in line with Data Subject's rights

We will only collect Personal Data to the extent that it is required for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

We will ensure that Personal Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties. You cannot Process Personal Data for any reason unrelated to your job duties.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with Youth for Christ's Data Retention Policy.

We will only Process in line with the Data Subjects' rights and in particular their rights to:

a. Withdraw consent to Processing at any time.
b. Request access to their Personal Data held about them.
c. Prevent our use of their Personal Data for direct-marketing purposes.
d. Ask to have inaccurate Personal Data amended.
e. Request the deletion or removal of Personal Data where there is no compelling reason for its continued Processing.
f. Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else.
g. Obtain and reuse their personal data purposes.

9. Data security

Youth for Christ will ensure that Personal Data is Processed securely and in line with its Information Security Policy.

10. Data accuracy

Every effort will be made to ensure Personal Data is accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. It must be relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out of date Personal Data.

11. Data retention and storage

Personal Data will only be stored and held in line with Youth for Christ's Data Retention Policy

12. Disclosure and sharing of Personal Data

Youth for Christ will not share Personal Data with third parties except for the reasons given in the next paragraph. This means Youth for Christ will not share or exchange the Personal Data it holds with other organisations.

We will share Personal Data if we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

13. Subject access requests

Data Subjects have a right to have a copy of all of their Personal Data we are holding. They need to make a formal request in writing. Youth for Christ will meet the request in full within one calendar month and no charge will be levied on anyone requesting their Personal Data.

The process for this is set out in the Subject Access Request Policy.

14. Transferring Personal Data to a country outside the European Economic Area (EEA)

We will only transfer any Personal Data we hold to a country outside the European Economic Area ("EEA") where the conditions of transfer provided for in the GDPR apply.

15. Data security breaches

The GDPR requires Data Controllers to notify to the applicable regulator and, in certain circumstances, to the Data Subject, any breach that may compromise the security confidentiality or integrity of Personal Data. The process to be followed is set out the in the Subject Access Request Policy.

16. Children's data

The GDPR requires that permission from a parent is required before a child's Personal Data can be Processed. The UK enactment of GDPR requires parental consent for children below the age of 13 years old.

Youth for Christ will ensure that parental permission will always be sought before Personal Data is collected and Processed for children below the age of 13 years old.

17. Privacy by design and Data Protection Impact Assessments DPIA)

We are required to implement privacy by design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner to ensure compliance with GDPR.

Data Controllers must also conduct DPIAs in respect of Processing likely to result in high risk to Data Subject for example:

a. where a new technology is being deployed;
b. where a profiling operation is likely to significantly affect Data Subjects; and
c. where there is Processing on a large scale of sensitive data.

If a DPIA indicates that the Processing is high risk, then the situation will need to be referred to the Data Processing Officer who will consult the ICO to seek its opinion as to whether the Processing operation complies with the GDPR.

18. Staff and volunteer training

All Youth for Christ staff and any volunteers required to access or handle Personal Data will be trained every two years in data protection good practice, and will be required to read this Privacy Standard as part of their induction. Staff will sign to say they have understood the Privacy Standard/ training and a copy will be kept in their HR file.

19. Privacy Notices

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects through relevant privacy notices ("Privacy Notices") setting out what Personal Data is held and Processed, the reasons for this and the legal basis together with how their rights in law are being upheld by Youth for Christ. Annex B set outs the requirements for a compliant Privacy Notice.

An appropriate Privacy Notice should also be readily available on all Youth for Christ websites.

20. Control and review

The Data Protection Officer for the national organisation will undertake a minimum of five data protection compliance checks with national staff on an annual basis and record results on the GDPR Data Compliance Checklist.

Similarly, the Data Protection Officers for each chartered ministry should undertake appropriate compliance checks with local staff and volunteers. The frequency of such checks should be decided by the local trustees and should be at least annually.

Any data protection issues requiring a decision will be recorded by the Data Protection Officer on the Data Protection Decision Log and stored securely.

21. Fundraising policy and practice

Our approach is to be legal, open, honest and respectful in all our fundraising activities. We do not engage in fundraising that might involve unreasonable intrusion on a person's privacy or is unreasonably persistent. Funds raised for a particular activity are used for that activity and our accounting system is designed to provide for this through a system of accounts for restricted funds. Youth for Christ do not use the services of professional or consultant/ freelance fundraisers and does not share its contact database with third parties. We are working to ensure that all our fundraising practices comply with the Code of Fundraising Practice issued by the Fundraising Regulator.

22. Responsibilities

Youth for Christ is responsible for and must be able to demonstrate compliance with the legal requirements and the principles set out above.

To ensure we meet these requirements, the key responsibilities are defined as follows:

a. National Trustees
   The national Trustees are responsible for ensuring that this Privacy Standard meets all the legal requirements and that it is implemented in the national organisation.

b. Centre Trustees
   Trustees of local chartered ministries (Youth for Christ 'Centres' and chartered projects) are responsible for ensuring that this core Privacy Standard is implemented in their chartered ministry.

c. Data Processing Officers

The Data Processing Officers, at national and local levels are responsible for and must be able to demonstrate compliance with the principles and policies set out in this document.

d. Staff and volunteers
Staff and volunteers are responsible for understanding and following the principles, practices and procedures set out for them by their Data Processing Officer through appropriate training.

23. Changes to this Privacy Standard

We reserve the right to change this Privacy Standard at any time. Where appropriate, we will notify Data Subjects any relevant changes affecting them.

DATA PROTECTION TERMS

Consent: Consent is the Data Subject giving permission for their private data to be Processed in a specific way. The GDPR sets a high standard for consent. It means offering individuals real choice and control. Consent requires a positive and unambiguous opt-in - not pre-ticked boxes or any other method of default consent. It should be linked to a clear statement of how the private data will used (set out in the Privacy Statement) and how the consent might be withdrawn or altered by the Data Subject at any time.

Data is information that is stored electronically, on a computer, or in paper-based filing systems.

Data Retention Policy: Youth for Christ's data retention policy which deals with the records and documents which Youth for Christ retain and/or dispose of, including electronic documents.

Data Subject: all living identified or identifiable individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their personal information, including those set out in the GDPR, Privacy of Electronic Communications Regulation (PECR) and the Fundraising Regulator's Code of Fundraising Practice.
Personal Data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal Data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data Controller means the people who or organisations that determine the purposes for which, the manner in which and the reason for which, any Personal Data is Processed. They are responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data used in our business for our own commercial purposes.
Data users are those of our employees whose work involves Processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data Processors include any person or organisation that is not a data user that Processes Personal Data on our behalf and on our instructions. Employees of Data Controllers are excluded from this definition but it could include suppliers that handle Personal Data on our behalf.

Data Protection Officer (DPO) – this is the person designated by Youth for Christ nationally or by one of its local chartered ministries as responsible for data protection and the implementation of this policy

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time. Personal Data is subject to the legal safeguards specified in the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when Youth for Christ collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or **Process** means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Sensitive Personal Data means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings, genetic data and biometric data where Processed to uniquely identify a person (for example a photo in an electronic passport). Sensitive personal data can only be Processed under strict conditions, including a condition requiring the express permission of the person concerned.

.

Your privacy notice checklist

What?

Decide what to include by working out:

- what personal information you hold;
- what you do with it and what you are planning to do with it;
- what you actually need;
- whether you are collecting the information you need;
- whether you are creating new personal information; and
- whether there are multiple data controllers.

If you are relying on consent, you should:

- display it clearly and prominently;
- ask individuals to positively opt-in;
- give them sufficient information to make a choice;
- explain the different ways you will use their information, if you have more than one purpose;
- provide a clear and simple way for them to indicate they agree to different types of processing; and
- include a separate unticked opt-in box for direct marketing.

Also consider including:

- the links between different types of data you collect and the purposes that you use each type of data for;
- the consequences of not providing information;
- what you are doing to ensure the security of personal information;
- information about people's right of access to their data; and
- what you will not do with their data.

Where?

Give privacy information:

- orally;
- in writing;
- through signage; and
- electronically.

Consider a layered approach:

- just in time notices;
- video;
- icons and symbols; and
- privacy dashboards.