Approved. YouthBorders Services Privacy Policy

This policy explains how YouthBorders uses, stores and protects any personal data it manages through the provision of its programmes and membership services.

YouthBorders takes its obligations to any personal data held very seriously and we are committed to protecting and respecting your privacy. The General Data Protection Regulation (GDPR) came into effect on 25 May 2018, this policy is written in accordance with GDPR.

We may update this policy from time to time to provide additional information or clarity. This Privacy Policy is part of a suite of policies which relate to data protection and privacy. The include:

- YouthBorders Services Privacy Policy (this policy)
- YouthBorders Data Protection Policy (contained within Employee Handbook)
- Employee Privacy Policy (contained within Employee Handbook)
- YouthBorders Website Privacy and Cookies Policy (embedded to our website)
- Job Applicant Privacy Notice (contained in our recruitment pack)

Our intention is to try and use plain English and youth work terminology as far as possible under our requirements for this policy. Any use of 'us', 'we' or 'our' etc. refers to YouthBorders. Any use of 'you', 'your' or 'you're' etc. refers to the user of our services. There are some legal terms used out of necessity but please get in contact if you require clarification on any of this policy.

If you have questions about what is set out below or would like to request a change in how we handle your personal data then please contact our Chief Officer, Susan Hunter at: susan@youthborders.org.uk

Data Protection Principles

1.Data is processed lawfully, fairly, and in a transparent manner.
2.Data is collected only for specified, explicit and legitimate purposes.
3.Personal data is processed only where it is adequate, relevant and not excessive.
4.Data kept is accurate and, where necessary, kept up to date or deleted without delay.
5.Personal data is not kept for longer than is necessary.
6.Personal data is processed in accordance with the data subject's rights.
7.The Charity adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised and unlawful processing, accidental loss, destruction or damage.
8.Data is not transferred to other countries without adequate protection.

Controller of Personal Data

Any personal information provided to or gathered by YouthBorders is controlled by YouthBorders, Scottish Charity Number: SC037680. A Company Ltd by Guarantee with Charitable Status: SC313338.

General Data Protection Regulation (GDPR)

GDPR is an evolution of the existing Data Protection Act (DPA) and Data Protection Directive. It is intended to give all of us greater visibility and control of our personal information (referred to as personal data).

Personal data is defined as, 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier."
What this means is any information an organisation holds that could possibly be used to identify a person, counts as personal data.

You can find out more about GDPR and how the Information Commissioner's Office (ICO) applies it to UK organisations on their website www.ico.org.uk

Child Protection and privacy

YouthBorders, like its members and many of its partners, operates in the youth sector, interacting with children and young people from aged 8 years. Where relevant, and if there exists a conflict, Child Protection legislation and policy supersede GDPR.

Types of information

Information, or data, that we hold is done so on a consent or legitimate interests basis, meaning that we hold and use information based on your permission (consent) to do so, such as providing your email address and name when you sign up to our email newsletter, or on the requirement for that information to provide our services (legitimate interests), such as through an application for funding or joining our network. There are three main types of information YouthBorders holds to provide services to you:

Information you give us:

You provide us with information when you use our services. This may be an application to join YouthBorders or registering for a training session we provide. In all cases, you choose to provide the information requested so that we may provide the service. Information will typically be provided to us via a form. This form may be accessed online, such as a membership application on our website, or via a physical form at or during a YouthBorders event, such as a registration form.

Information that technology gives us:

Information is sometimes automatically passed between your chosen technology and YouthBorders' technology by accessing our digital services. The most common usage is

website analytics and browser cookies.

Your web browser automatically passes information about itself and your device (computer/mobile etc.) to any internet location you visit. Your browser has specific settings you can adjust to limit or increase these options.

This information is often referred to as metadata and is information including log data, information passed by your web browser like IP address or other web browser information; device information, like what type of computer or mobile device accessed our website; location information, such as an approximate location while accessing our website. Our website has its own privacy policy which tells users exactly what information is being collected by the website.

Electronic communications:

We maintain an active email bulletin service to opted-in users, this service operates an independent op-out, meaning you may unsubscribe without having to contact us.

How information is used

We use any information you provide to us to fulfil the service or services related to your information. For example, to apply for membership, we will ask for the information about your youth group, meeting place, contacts and other information that we require to grant membership, according to Youth Scotland's and our membership criteria. Likewise, we will ask for names, contact details, dates and times when you book a training event, so that we know who will attend and when.

In essence, the information is directly related to being able to fulfil the service we set out to provide to you or that is required by law. The core uses of personal data held by YouthBorders are:

- To provide, update, maintain and improve our services
- As required by law, legal process or regulation
- To communicate and respond to requests, comments and questions
- To send service emails and other communications essential to providing membership and services
- For billing, account management and other administrative matters
- To maintain security and standards
- To recruit volunteers, trustees or staff to our organisation

In addition to the core purpose, we use data for, we may also use information to analyse or profile our users to fulfil legal obligations, reporting obligations and to maintain and improve our services. This may include:

- We may use data to analyse our services e.g. satisfaction surveys and programme evaluation surveys to see how we are doing and take on board feedback
- We may profile data on a geographic basis e.g. we may look at whether a group will qualify for funding or programme access due to relevant geographic criteria

- We may profile data on age or gender basis e.g. we occasionally seek to understand our membership demographics to improve our offering and complete our annual reporting
- We may profile data for aggregated statistics to complete reports e.g. we are often required to complete annual reports for programmes we run as a contractual obligation

Sharing information

We do not provide any personal information to third parties for commercial purposes, so we will never rent or sell your personal information.
Some YouthBorders programmes, events or activities are supported or funded by other organisations. These programmes and events can require that reporting, financial and evaluation data be shared with the supporting funder or partner as a condition of contract or that it is required or authorised to do so by law. We will always make you aware of where this applies.

The current obligations on YouthBorders are as follows:

Membership (including insurance applications)

"Membership" is a joint membership of YouthBorders and Youth Scotland. Membership data primarily contains data of member groups, but this does include personal data relating to member contacts (e.g. email or phone numbers of lead volunteers).

Personal data from direct memberships and applications go directly to Youth Scotland, this membership data is shared with YouthBorders through a CRM which YouthBorders accesses. Some basic group contact details are shared with Law At Work (LAW) so that members may gain access to the legal advice service benefit of their membership package. See LAW privacy statement for details.

All member groups who apply for an insurance package have group data and meeting address details, but not contact details, submitted directly to the Insurance Brokers, who submit to the Insurance Providers. The Insurance Brokers are Towergate Insurance.

YouthBorders Worker Training

YouthBorders offers training to our members through Youth Scotland, when Youth Scotland are the trainer we will share personal information and data on participants undertaking the training with them such as email addresses, phone number, support needs. For all other training YouthBorders remains the host and no personal data is shared.

PVG Scheme

All staff, trustees and volunteers who apply for PVG scheme membership/updates provide sensitive personal data required to process the PVG Checks. These details are submitted by YouthBorders directly to Volunteer Scotland. Volunteer Scotland produce PVG certificates and share these with applicants and with YouthBorders.

Security and where information is stored

YouthBorders takes every reasonable precaution to ensure any data we hold is secure and stored according to GDPR. The following details explain the groupings for data storage; the technology involved and location. In addition to the secure storage outlined below, access to any YouthBorders system is always protected by the requirement for secure login to our systems. Any physically held data is protected locally by secure entry system and alarm. Filing cabinets where used are locked.

Membership data

Our membership data is stored, accessed and updated in a Microsoft Dynamics 365 CRM system operated by Youth Scotland. Dynamics 365 is a third-party, cloud-based system and data is not stored locally. Microsoft datacentres are among the most secure in the world and are held in European GDPR-compliant datacentres. When required our membership data is transferred from Dynamics in to the YouthBorders Office 365 system.

Website

The YouthBorders websites are hosted on 'And We Do This Ltd'. No data is held locally and is all held in European GDPR-compliant datacentres. Please refer to the Privacy & Cookies Policy for our website.

Eventbrite

YouthBorders uses the Eventbrite platform to manage our bookings for training and events. Eventbrite is a third-party, cloud-based system and data is not held locally. Eventbrite store data globally in compliance with GDPR and the EU-US Privacy Shield Framework.

Office 365 Suite

YouthBorders uses Microsoft Office 365 suite, a hosted, online version of Microsoft Office software. Within Microsoft 365 we use Excel, Word, Forms, Outlook, SharePoint and Teams. Microsoft Office 365 suite is Microsoft compliant with GDPR and privacy standards such as the world's first international code of practice for cloud privacy, ISO/IEC 27018.

MailChimp

We use MailChimp as our email newsletter platform. MailChimp is a third-party, cloud-based system and data is not held locally. MailChimp store data in the USA in compliance with GDPR and the EU-US Privacy Shield Framework.

Doodle Poll

We use Doodle Poll as our meeting timetabling platform. Doodle Poll is a third-party, cloud-based system and data is not held locally. Doodle poll store data in the USA in compliance with GDPR and the EU-US Privacy Shield Framework.

WhatsApp

YouthBorders use WhatsApp, a multiplatform messaging app as a method of communication with members. WhatsApp is not GDPR compliant and as part of the Facebook group there are concerns about data storage and security. Members who choose to join the WhatsApp group will be made aware of the security limitations and asked to agree to a set of terms of use. YouthBorders will continue to use WhatsApp whilst we review options for an alternative.

Norcox RAG Journal

YouthBorders use the Norcox RAG Journal to support the deliver of our Stepping Stones project. Rag Journal is provided by Norcox Solutions Ltd, who are registered with the Information Commissioners Office as a Data Controller for the purposes of the Data Protection Act and GDPR legislation. The data is stored in the Microsoft Cloud (Azure), in datacentres physically located in the EU (Amsterdam and Dublin).

Data retention

YouthBorders will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

To achieve this, we have grouped personal data and set the following general limitations:

Membership data

Membership data is considered active and current during a membership period of 12 months. Data held by Youth Scotland and YouthBorders will be done so for up to 24 months after non-renewal before being archived. Only the base data required to identify a returning member group will be archived.

Project data

Projects and programmes run for varying periods of time, typically increments of 12 months by financial year. To accommodate this, we will keep data for period of time limited by project completion dates or by financial year in rolling projects.

Data is considered active and current during a project. Data will be held by YouthBorders for up to 24 months from the project completion date or 24 months from financial year end for rolling programmes.

Training and event registration data

YouthBorders uses personal data to allow participants to register for training and other event opportunities. This is typically through the Eventbrite booking platform but occasionally through direct communication with YouthBorders (forms and emails etc.)

Data will be held by YouthBorders for up to 36 months from the training or event completion date.

Financial data

Like other organisations, YouthBorders is required to hold organisational financial records for accounting, auditing and taxation purposes. Data will be held by YouthBorders for up to 84 months from the end of financial year.

Employee, Volunteer and Trustee data

YouthBorders holds various personal data on current and former employees and trustees. Data is considered active and current during the period an employee is actively employed by the organisation or for the tenure of a trustee. Data will be held by YouthBorders for up to 12 months for employees and trustees and 12 months from last contract for freelancers and contractors.

Job Applicants

For more details, please refer to our 'YouthBorders Job Applicant Privacy Notice'.

PVG member applicant data

YouthBorders holds personal data on PVG Applicants whilst their PVG Scheme application is being processed and until their PVG Certificate has been received and a recruitment decision made by the member group. After a recruitment decision has been made, we will securely destroy the PVG Certificate. We will retain minimal contact details and note of PVG certificate number on file for the duration of their active involvement with a YouthBorders Member Group in a regulated work role. Please refer to 'YouthBorders PVG Secure handling policy' for more details. *These limitations may be superseded by legal requirements placed upon YouthBorders.*

Cookies

Like the majority of websites, the YouthBorders website uses modern technology and data provided by you and your browser to try and provide the best service and experience we can.

Cookies may be used on our website. A cookie is a very small text file that is placed on your computer's hard drive when accessing a website and it collects standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity.

You can set your browser to refuse cookies and you can find out more information on how to refuse and delete cookies at http://www.aboutcookies.org. However, please note that some of this website may not function as a result.

Individual rights

GDPR provides certain rights for individuals. These are how they apply to YouthBorders:

1. The right to be informed – the core purpose of this policy; we aim to tell you about the collection of personal data.
2. The right of access – you have access to your personal information (often called a "data subject access request"). This enables you to ask for a copy of the personal information we hold about you. This is normally free but please note that, as per ICO guidelines, an administration fee may apply, "when a request is manifestly unfounded or excessive, particularly if it is repetitive."
3. The right to rectification – in clearer words, the right to have corrections made. This a shared obligation between us to keep personal data as up to date as is practical.
4. The right to erasure - this enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
5. The right to restrict processing - This enables you, where appropriate, to ask us to suspend the processing of personal information about you. For example, if you are checking the accuracy of information we hold.
6. The right to data portability – in clearer words, the ability for you to take personal data from us to an alternative supplier. Less relevant to our operations but the right remains.
7. The right to object - where we are using a legitimate interest basis and there is something which makes you want to object to processing on these grounds. This may mean we are unable to provide some services to you.
8. Rights in relation to automated decision making and profiling - automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

Data Retention Reference Guide

Membership Data	24 months after non-renewal
Training and Events Data	36 months from event/training taking place
Project or Programme Data	24 months from completion of project or as specified in terms of grant
Financial Data	84 months
PVG Data	For as no longer than necessary
Job Applicant Data	6 months following completion of recruitment, or earlier if requested.
Employee Data	See Employee Handbook for details