

Bank Youth Project

Data Protection Policy 2019 (reviewed in March 2022)

Note: This policy should be read in conjunction with the BYP's Internet Access Policy for Young People and Staff Members; a part of the Child Protection Policy.

1. Legislation and Purpose of the Policy

Data protection is the fair and proper use of information about people. It is part of the fundamental right to privacy – but on a more practical level, it's about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others and striking a balance with the wider interests of society.

On 25 May 2018 the General Data Protection Regulations (GDPR) came into full power, as a part of the Data Protection Act 2018 (DPA 2018) which replaces the previous Data Protection Act 1998 (DPA 1998). Part 2 Chapter 2 of the DPA 2018 supplements and tailors the GDPR. For the BYP, this is the part that applies. It sets out the key principles, rights and obligations for most processing of personal data.

2. Sources.

This policy has been compiled in accordance with published guidance from the Information Commissioner's Office (ICO) available at ico.org.uk/for-organisations/charity – accessed 16 January 2019.

3. Compliance

In order to be compliant the BYP must ensure that any personal data that we collect or keep a record of is maintained in accordance with these seven key principles. Data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation').
- 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 or organisational measures ('integrity and confidentiality').

4. Controller and Data Protection Officer.

A new principle of accountability under GDPR specifically requires the BYP to take responsibility for complying with the seven key principles and to have appropriate processes and records in place to demonstrate that we comply, in the role of Controller (see

"Definitions" at Annex A). The Chairman of the BYP Management Group is the Controller for the BYP. The BYP's Data Protection Officer is the Administrator.

5. Consent

The GDPR introduces the rule that an indication of consent to hold and to process personal data must be unambiguous, freely given and involve a clear affirmative action (an opt-in), as well as a specific right for consent to be withdrawn. If existing consents meet the GDPR standard, they do not need to be renewed.

Consent documentation must therefore:

- Be prominent, concise, separate from other terms and conditions and easy to understand.
- Include the BYP's name; contact details for the Controller and the Data Protection Officer.
- Explain why we want the data.
- Explain what we will do with it and for how long it will be kept.
- Make it clear that individuals can withdraw consent at any time.
- Explain the other rights of individuals (see Para.6 below).
- Show how to lodge a complaint about holding personal data.

A Consent Information Statement covering the main principles is at Annex B. It does not go into great detail, as it is important that it be readily usable, clear and easy to understand. Nonetheless, all data subjects must be aware of their rights under GDPR and staff must be prepared to answer reasonable questions about the legislation or refer the individual to the Data Protection Officer.

Consent forms will be retained under the same provisions of GDPR as any other data.

6. Rights of individuals (data subjects)

The GDPR provides the following rights for individuals:

- **The right to be informed.** This is covered by consent (see Para.5 above) but must be updated as soon as anything changes.
- **The right of access.** Individuals have the right to access their personal data. This is commonly referred to as subject access. Individuals can make a subject access request verbally or in writing. The BYP has one month to respond to a request and will not charge a fee to deal with it. Note: An exemption to this right may apply if serious harm to the mental or physical health of the data subject may occur. If in doubt, check with the Data Protection Officer.
- **The right to rectification.** The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. The BYP has one calendar month to respond to a request.
- **The right to erasure.** The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. The BYP has one month to respond to a request.
- **The right to restrict processing.** When processing is restricted, we are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. The BYP has one month to respond to a request.
- **The right to data portability.** The right to data portability allows individuals to obtain and reuse their personal data for their own purposes.

- **The right to object.** The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances; for example, individuals have an absolute right to stop their data being used for direct marketing. An individual can make an objection verbally or in writing. The BYP has one month to respond to an objection.
- **Rights in relation to automated decision making and profiling.** These are unlikely to apply to the BYP.

7. Personal Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (which will usually be the Information Commissioner's Office – ICO). We must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay. We must have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the ICO and the affected individuals. We will also keep a record of any personal data breaches, regardless of whether or not we are required to notify.

8. Data Protection best practice.

The following practices will help to ensure that the BYP complies with GDPR:

Tell people what we are doing with their data. People should know what we are doing with their information and who it will be shared with. This includes the young people, staff and volunteers. This is a legal requirement, as well as established best practice and requires the consent of the data subjects.

Make sure our staff and volunteers are adequately trained. New employees must receive data protection training to explain how they should store and handle personal information. Refresher training will be provided at regular intervals for existing staff and volunteers.

Have a clear, unambiguous and easy-to-understand consent procedure. Records of consent must be kept in accordance with GDPR. See Annex B.

Use strong passwords. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep our information secure from would-be thieves.

Encrypt all portable devices. We will make sure that all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

Only keep people's information for as long as necessary. The BYP will have established retention periods in place and a process for deleting personal information once it is no longer required.

Regularly review all data protection practices. The BYP will regularly review and, where necessary, update our privacy information. If we plan to use personal data for a new purpose, we will update our privacy information and communicate the changes to individuals before starting any new processing.

Act upon data breaches promptly. The Data Protection Officer and, if necessary, the Controller must be informed at once if a data protection breach is suspected. They will be able to advise on what steps need to be taken.

8. Policy review and signatures

This policy will be reviewed not less frequently than annually.

Date this policy was last reviewed: 14.03.2022

Date of next review: March 2024

Signed by the Chair of the Management Group (Controller):.....

Signed by the Administrator (Data Protection Officer).....



Annex A

Definitions

Personal Data

Personal data means information about a particular living individual. This might be anyone, including young people (members), senior helpers, volunteers, staff, trustees and members of the Management Group or a member of the public. It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data. Any data on electronic media and/or organised in a systematic way is relevant here.

Processing

Almost anything we do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

Controller

A controller is the person or organisation that decides how and why to collect and use the data. The controller must make sure that the processing of that data complies with data protection law.

Data Subject

A Data Subject is the technical term for the individual about whom particular personal data is held.

Data Protection Officer

Responsibility for the day to day administration of GDPR lies with the Data Protection Officer.

Annex B

Consent Information

The following information shall be provided to every person connected with the BYP before they become a data subject:

“As a part of its work, the BYP collects and records data about its members. This includes information such as your name, age and gender, as well as records of how often you attend and topics that have been discussed. This information helps the BYP to improve its services and to analyse data in support of fundraising to help the sustainability of the project. Only the minimum information necessary for these purposes will be collected.

The proper control and security of this information is written in law as the General Data Protection Regulations (GDPR), which is a part of the Data Protection Act 2018. The BYP’s Data Protection Officer (the Administrator) is responsible for the day-to-day working of these rules. Overall control of these rules within the BYP rests with the Chairman of the Management Group. If you have a complaint about how information about you is being used, you can bring this, either in writing or verbally, to either of these responsible people. You are entitled to a response within one month.

Information about you can only be collected with your permission. You have the right to see any information about you that the BYP holds. You have the right to have any wrong information put right and to have all information about you erased after you are no longer a member of BYP. You can withdraw your permission at any time.

Information about you will only be held for as long as is necessary to support the work of BYP. This is reviewed regularly.

If you wish for more information about data protection, or if you wish to read the full BYP data protection policy document, please ask a member of staff.”