Braintree Youth Project Charity

General Data Protection Regulation

BYPC is the data controller under the GDPR and is ultimately responsible for implementation of the GDPR.

The Data Protection Officer, who provides BYPC's primary contact to the Information Commissioner, and is responsible for ensuring provision of suitable GDPR advisory, training and awareness services, GDPR request handling, ensuring compliance with Information Commissioner actions, and for keeping the Board of the Charity aware of relevant GDPR issues.

BYPC aims to ensure that all personal data held is in accordance with the General Data Protection Regulation (GDPR).

This document sets out how BYPC intends on dealing with data.

Aims

The aims of this policy are to ensure:

- That staff, volunteers and users of BYPC understand that any data we hold on them is in a safe secure place and not to be shared outside of any legal requirements without their prior consent.
- BYPC will have procedures in place to deal with:
    - Subject Access Requests
    - Erasure requests

Data Protection with the GDPR

BYPC has a requirement to take personal data for its young people and their parents in order to be able to contact them appropriately, this data should all be kept on the BYPC portal and 'Run a Club' which uses encrypted cloud servers and has GDPR Compliance.

All Data should be filed in appropriate folders.

Any other person data which is in written or printed form should be locked away in the main office.

Braintree Youth Project Charity

General Data Protection Regulation

Procedure for:

Subject Access Request:

1. Establish that the request is in fact a subject access request.
    a. This may mean going back to the person and making sure that you have correctly understood what they have asked for and that they are making a subject access request for all of their personal data.
    b. Always make sure that the request is in writing.
    c. We will also need to know if the person requesting the data wishes to have their digital data in a digital format or printed.
2. Inform the person who requested the data that we will comply with the request and give the applicant an estimated time that it will take to compile their data together. If data is printed they will need to know how much a printed copy of everything is likely to cost.
3. Go to the portal and find the digital files we hold on that person and make a copy of them for the person to have. This could be either printed or given digitally to them.
4. Ensure that any legal data which we are not allowed to pass on is not passed on and that all data we are legally allowed to pass on is filed.
5. Ensure that the personal data is given fully as requested and in a reasonable amount of time.
6. Ask the person to sign a form saying that they have received a copy of their personal data. Give a copy to the requester and keep the original on file.
7. Fill in a form on the portal of the Subject access request, date requested, date completed and any additional information which is appropriate.

Erasure request

1. Establish that the request for erasure is correct
2. Check all of the data that we currently hold on the person making the request
3. Any data which we are not legally required to hold can be deleted or shredded
4. Sign a form saying that the Erasure request has been completed and that we have complied with their request. Ensure that the form is dated.
5. Fill in a form on the portal for the Erasure request, date requested, date completed and any additional information which is appropriate. If there is any data we hold which we are legally not allowed to erase, double check how long we have to retain that data and if the person in question is allowed to see that data. If they are not allowed to see it then we can say we have some items of data which we legally have to keep but everything else has been deleted.

Approved: Sept 2018