Data Protection Policy

11th September 2019

Contents

1. Purpose of the policy

1.1 Football Beyond Borders ("we") are committed to complying with privacy and data protection laws including:

a. the General Data Protection Regulation (“the GDPR”) and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Act 2018;

b. the Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003;

and

c. all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the Information Commissioner’s Office (“ICO”) or any other supervisory authority.

(together "the Legislation")

1.2 This policy sets out what we do to protect individuals' personal data.

1.3 Anyone who handles personal data in any way on behalf of Football Beyond Borders must ensure that they comply with this policy. Section 3 of this policy describes what "personal data" is. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

1.4 This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

2. About this policy

2.1 The types of personal data that we may handle include details of: students, staff members (both of Football Beyond Borders and schools who we work with), trustees, patrons, donors, marketing prospects, sub-contractors and volunteers.

2.2 Jack Reynolds is the Director and Data Protection Contact at Football Beyond Borders and is responsible for ensuring compliance with the GDPR and with this policy. Any questions or concerns about this policy should be referred in the first instance to the Data Protection Contact who can be contacted on jreynolds@footballbeyondborders.org or on 07969 523 766.

3. Definitions of data protection terms

3.1 The following terms will be used in this policy and are defined below:

3.2 Data Subjects include all living individuals about whom we hold personal data, for instance an employee or a supporter. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 Personal data means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.4 Data controllers are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They are, in effect, in charge of the information that is collected and have a responsibility to process personal data in compliance with the Legislation. Football Beyond Borders is the data controller of all personal data that we manage in connection with our work and activities.

3.5 Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf. An example of Football Beyond Borders' data processors is email marketing providers (such as MailChimp).

3.6 European Economic Area includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.7 ICO means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

3.8 Processing is any activity that involves the use of personal data, whether or not by automated means. It includes but is not limited to doing any of the following in respect of any personal data:

a. collecting;
b. recording;
c. organising;
d. structuring;
e. storing;
f. adapting or altering;
g. retrieving;
h. consulting;
i. using;
j. disclosing by transmission;
k. disseminating or otherwise making available;
l. alignment or combination;
m. restricting;
n. erasing; or
o. destruction.

3.9 Sensitive personal data (which is defined as "special categories of personal data" under the GDPR) includes information about a person's:

a. racial or ethnic origin;
b. political opinions;
c. religious, philosophical or similar beliefs;
d. trade union membership;
e. physical health or mental health or any other health condition;
f. sexual life or orientation;
g. genetic data;
h. biometric data; and
i. such other categories of personal data as may be designated as "special categories of personal data" under the Legislation.

4. How should you approach data protection matters?

4.1 Familiarise yourself with our data protection policies, privacy notices and privacy statements. These documents outline how and for what purposes we process student, parent and third party data.

4.2 Always consider data protection issues as early as possible during the planning stages for any new operation, product, service or technology.

4.3 A key requirement of the GDPR is for us to demonstrate our compliance with our data protection obligations. Therefore, any decisions made about data protection or processing activities should be sufficiently documented and recorded on our systems for others to access.

4.4 Always remember that an honest analysis or answer is required and if the answer to a particular question is "I don't know" or "I'm not sure", this should be documented.

4.5 Anyone accessing personal data should ensure that they understand the six data protection principles under GDPR (summarised below) and are able to recognise a data subject access request (**DSAR**). You should contact the Data Protection Contact if you receive a DSAR or become aware of security breach.

5. Data protection principles

5.1 We are required to comply with these principles and show that we comply with them in respect of any personal data that we deal with as a data controller.

5.2 Personal data should be:

a. processed fairly, lawfully and transparently;
b. collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;
c. adequate, relevant and limited to what is necessary for the purpose for which it is held;
d. accurate and, where necessary, kept up to date;
e. not kept longer than necessary; and
f. processed in a manner that ensures appropriate security of the personal data.

6. Processing data fairly and lawfully

6.1 The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied. This includes where the data subject has given consent for their data to be processed in a certain way or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract or necessary for the purposes of the controller's legitimate interests (e.g. we need to process personal data to be able to run our programme).

6.2 To comply with this principle, every time we receive personal data about a person directly from that individual, which we intend to keep, we need to provide that person with "the fair processing information". In other words, we need to tell them:

a. the type of information we will be collecting (categories of personal data concerned);

b. who will be holding their information, i.e. Football Beyond Borders including contact details and the contact details of our Data Protection Contact (if we have one);

c. why we are collecting their information and what we intend to do with it, for instance to process donations or send them mailing updates about our activities;

d. the legal basis for collecting their information (for example, are we relying on their consent, or on our legitimate interests or on another legal basis);

e. if we are relying on legitimate interests as a basis for processing, what those legitimate interests are;

f. whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;

g. the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;

h. details of people or organisations with whom we will be sharing their personal data;

i. if relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards;

j. the existence of any automated decision-making including profiling in relation to the personal data; and

k. their various rights under the Legislation which are set out at section 11 below.

6.3 Where we obtain personal data about a person from a source other than the person his or her self, we must provide that individual with the following information in addition to that listed under 6.2 above:

a. the categories of personal data that we hold; and

b. the source of the personal data and whether this is a public source.

This information must be provided to the data subject:

c. within a reasonable period of time, being no later than one month from when we obtained the relevant personal data,

d. if we are using the data to communicate with the individual, the date that we first get in touch with that data subject or,

e. if we need to disclose this personal data to a third party, at the same time as the first disclosure.

6.4 In addition, in both scenarios, (where personal data is obtained both directly and indirectly) we must also inform individuals of their rights outlined in section 11 below, including the right to lodge a complaint with the ICO, and the right to withdraw consent to the processing of their personal data.

6.5 This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

7. Processing data for the original purpose

7.1 The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we obtained their information.

7.2 This means that we should not collect personal data for one purpose and then use it for another unless the new purpose is compatible with the original purpose for which data was processed.

If it becomes necessary to process a person's information for a new purpose, the data subject should be informed of the new purpose beforehand. For example, if we collect personal data, such as a contact number or email address, in order to update a person about our activities, it should not then be used for any new purpose, for example to share it with other organisations for marketing purposes or for adding to our marketing database, without first getting the data subject's consent.

8. Personal data should be adequate, accurate and limited to what is necessary

8.1 The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant.

8.2 Data should be limited to what is necessary in relation to the purposes for which it is processed.

8.3 We should take reasonable steps to ensure that inaccurate or out-of-date data is either destroyed securely or corrected.

9. Not retaining data longer than necessary

9.1 The fifth data protection principle requires that we should not keep personal data for longer than we need to achieve the purpose it was collected for. This means that the personal data that we hold should be securely destroyed or erased from our systems when it is no longer needed.

9.2 If you think that we are holding out-of-date or inaccurate personal data, please speak to the Data Protection Contact.

9.3 For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please contact the Data Protection Contact or seek legal advice.

10. Data security

10.1 The sixth data protection principle requires that we keep secure any personal data that we hold.

10.2 We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

10.3 When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device it should always be encrypted.

10.4 When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

10.5 The following security procedures and monitoring processes must be followed in relation to all personal data processed by us:

a. the pseudonymisation (i.e. processing data in a way so that it cannot be linked to a specific data subject without additional information) and encryption of personal data;

b. measures to restore availability and access to data in a timely manner in event of physical or technical incident;

c. process for regularly testing, assessing and evaluating effectiveness of security measures;

d. backing up data (daily back-ups should be taken of all data on the system and data should not be stored on local drives or removable media as these will not be backed up);

e. entry controls (any stranger seen in entry-controlled areas should be reported);

f. staff should ensure that individual monitors do not show confidential information to passers-by and that they lock / log off from their PC when it is left unattended;

g. paper documents should be shredded, memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required;

h. personal data must always be transferred in a secure manner (the degree of security required will depend on the nature of the data – the more sensitive and confidential the data, the more stringent the security measures should be);

i. other measures to ensure confidentiality, integrity, availability and resilience of processing systems;

j. desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential); and

k. staff must keep data secure when travelling or using it outside the offices.

11. Rights of individuals under the GDPR

11.1 The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of Football Beyond Borders needs to be aware of these rights. They include (but are not limited to) the right:

a. to request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known a subject access rights). This is a DSAR.;

b. to be told, where any information is not collected from the person directly, any available information as to the source of the information;

c. to be told of the existence of automated decision-making;

d. to object to the processing of data other than where the processing is based on either the conditions of public interest or legitimate interests;

e. to have all personal data erased (the "right to be forgotten") unless certain limited conditions apply. This right exists where, for example, it is no longer necessary to hold

personal data, the data subject withdraws their consent or personal data has been unlawfully processed;

f. to restrict processing where the individual has objected to the processing; and

g. to have inaccurate data amended.

12. Transferring data outside the EEA

12.1 The GDPR requires that when organisations transfer personal data outside the EEA, they take steps to ensure that the data is properly protected.

12.2 The European Commission has determined that certain countries already have adequate data protection regimes in place. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, but this list may be updated.

12.3 As such, personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation in the EEA. In transferring personal data to other countries outside the EEA (which are not on this approved list), it will be necessary to enter into an EC-approved agreement, seek the explicit consent if the individual, or rely on one of the other derogations under the GDPR that apply to the transfer of personal data outside the EEA.

12.4 The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the Data Protection Contact before transferring personal data to organisations in the US.

12.5 For more information, please speak to the Data Protection Contact or seek further legal advice.

13. Processing sensitive personal data

13.1 On some occasions we may collect information about individuals that is defined by the GDPR as special categories of personal data, and special rules will apply to the processing of this data. In this policy we refer to “special categories of personal data” as “sensitive personal data”. The categories of sensitive personal data are set out in the definition in Section 3.9.

13.2 Purely financial information is not technically defined as sensitive personal data by the GDPR. However, particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously.

13.3 In most cases, in order to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information, we will also have to be absolutely clear with people about how we are going to use their information.

13.4 It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please speak to the Data Protection Contact.

14. Notification

14.1 We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the GDPR, we will consult with the ICO where necessary when we are carrying out "high risk" processing.

14.2 We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours of becoming aware of them. We will also notify affected individuals, without undue delay, where the breach is likely to result in a high risk to the rights and freedoms of these individuals.

14.3 We have to keep a record of any data breaches. As such, if you think a data breach has occurred, please immediately get in touch with the Data Protection Contact and let them know when the breach occurred, when you became aware of the breach and what the breach is. Our Data Protection Contact will then liaise with you to understand the significance of the breach and whether it needs onwards reporting to the ICO and/or the data subject.

15. Monitoring and review of the policy

15.1 This policy is reviewed annually by our Executive Leadership Team to ensure that it is achieving its objectives.

Approved: 13th September 2019

Next Review Date: 13th October 2020