

## 6.5 Data Protection Policy

- **Introduction**

The Data Protection bill will replace the Data Protection Act (1998) and becomes enforceable beginning 25 May 2018

GDPR applies to how and why data is processed. It aims to give control back to citizens over their personal data and unify regulations within the EU. In addition, it places significantly more legal liability on the organisation (data controller) in relation to any breach. The legislation requires that each organisation shall be responsible for and be able to demonstrate, compliance with the principles. Information that applies to the GDPR is:

- Personal Data (Information relating to an individual whether it relates to his / her private, professional or public life – it can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking sites, medical information or an IP address.
- Sensitive Personal Data (Genetic data and biometric data that uniquely identifies an individual)

This policy has been written to guide staff and sets out the protocol for processing personal data and safeguarding individual's rights. Designed to help and encourage all employees of the company to achieve and maintain standards of conduct in their work in complying with GDPR legislation on behalf of The Braunstone Foundation (trading as b-inspired Ltd).

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes: further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and where necessary, kept up to date: every reasonable step must be taken to ensure personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 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 freedoms of individuals.

- 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.

Managers are responsible for ensuring that staff observe the standards set for working with personal data and should be able to demonstrate due diligence to customers, suppliers, volunteers and other contacts on behalf of the company.

The policy is subject to regular review to reflect, for example, changes to legislation or to the structure or amended policies of the Braunstone Foundation.

All staff are expected to apply the policy and to seek advice from their line manager when required.

## • **Implementing GDPR**

The Braunstone Foundation needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective individuals within the community, The Braunstone Foundation's own employees, suppliers, students and others with whom The Braunstone Foundation conducts business. In addition, the Braunstone Foundation may occasionally be required by law to collect and use certain types of personal information to comply with the requirements of government departments, funding authorities and the Charities Commission. This personal information must be dealt with properly – whether it is collected on paper, electronically, or other means.

The Braunstone Foundation considers the lawful and correct treatment of personal information as important to the achievement of our objectives and to the success of our operations, in order to maintain confidence between those with whom we deal and ourselves.

Our data policy sets out our commitment to protecting personal data and how we safeguard and implement that commitment with regards to the collection and use of personal data ensuring it complies with GDPR

## **Processing Data**

Within GDPR, there is a distinct difference between business to consumer (B2C) and Business to Business (B2B) marketing. Under GDPR, there are six equally valid grounds to process personal data:

The lawful basis for processing data are:

- The data subject has given consent to the processing of his/ her personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority
- Processing is necessary for the purpose of the legitimate interests pursued by the controller.

There are two of these that are relevant to direct B2B marketing, they are *consent* or *legitimate interest*. GDPR states that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

Using *legitimate interest* as the basis for B2B marketing involves ensuring key conditions are met:

- The processing must relate to the legitimate interests of your business or a specified third party, providing that the interests or fundamental rights of the data subject do not override the businesses legitimate interest.
- The processing must be necessary to achieve the legitimate interests of the organisation.

## **Right of Access**

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why we are using their data, and check it is being done lawfully.

Individuals have the right to obtain the following:

- Confirmation that we are processing their personal data;
- A copy of their personal data; and other supplementary information – this largely corresponds to the information that is provided in a privacy notice.

## **Personal data of the individual**

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that we establish whether the information requested falls within the definition of personal data.

In addition to a copy of their personal data, we also have to provide individuals with the following information:

- the purposes of processing;

- Categories of personal data concerned;
- Recipients or categories of recipient you disclose the personal data to;
- Retention period for storing the personal data or, where this is not possible, criteria for determining how long it will be stored.
- Confirmation of the right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- The existence of automated decision-making (including profiling); and
- Safeguards you provide if Data is transferred.

An individual can make a subject access request verbally or in writing. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point. The GDPR does not prevent an individual making a subject access request via a third party. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request.

A request does not have to include the phrase 'subject access request' as long as it is clear that the individual is asking for their own personal data.

All requests received whether verbal or in writing should be recorded on the form contained in this policy, dated and forwarded to the Head of Operations.

All requests received must be acted on at the latest within one month of receipt.

This timeframe can be extended by a further two months if the request is complex or the organisation has received a number of requests from the individual. The organisation must let the individual know within one month of receiving their request and explain why the extension is necessary.

If you have doubts about the identity of the person making the request - ask for more information. However, it is important that you only request information that is necessary to confirm identity.

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The organisation does not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

The other individual has consented to the disclosure; or it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, the organisation must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;

In the event that a request is manifestly unfounded or excessive The Braunstone Foundation will charge an administration fee and will not comply with the request until the fee has been received.

- **Control of Data**

- **Staff responsibilities**

- Braunstone Foundation staff should acquaint themselves with the data protection policy and abide by recognised good practice in regard to data protection principles.
- Service Managers shall act as point of contact in ensuring that staff understand how to conform to the required standard. Ensuring that in any data captured complies with and is treated in accordance with the act.
- Head of Operations will ensure that adequate training and support is made available for all staff responsible for personal data, and ensure that staff know where to find/obtain further guidance ensuring that both internal and external queries about data protection, to the organisation, are dealt with effectively and promptly and individuals rights in regard to safeguarding data and the individual's right to inspect personal data are adhered to.
- The company will regularly review data protection procedures and guidelines.

- **Best –Practice Guidelines for employees of The Braunstone Foundation**

- Acquisition of personal data. - Those wishing to obtain personal data must comply with guidelines issued from time to time by The Company and in particular:
  - Should outline to data subjects the purpose (s) for which they are gathering data, obtaining their explicit consent, and inform them that The Braunstone Foundation will be the controller for the purposes of GDPR. In addition, data subjects should be aware of any other persons/organisations to whom the data may be disclosed.
  - If personal data is collected, explicit consent is not only best practice, it is mandatory. No more data should be collected than is necessary for the purpose(s) declared.

- Holding / safeguarding / disposal of personal data
  - Data should not be held for longer than is necessary. For further information please see The Braunstone Foundations document retention policy or contact your line manager for guidance.
  - Personal data should be reviewed periodically to ensure it is up to date and accurate and to determine whether retention is necessary.
  - Where possible, personal data should be anonymised.
  - Adequate measures should be taken to safe guard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures that need to be taken.
  
- Processing of personal data
  - In this particular context “processing is used in the narrow sense of editing, amending or querying data. In the context of the Act as a whole “processing” is very widely defined to include acquisition, passive holding, disclosure and deletion.
  - Personal data must not be processed except for the purpose (s) for which it was obtained or for a similar analogous (i.e. performing similar functions). If the new purpose is very different, the data subjects consent must be obtained.
  
- Disclosures and transfer of personal data

The Braunstone Foundations policy is to exercise discretion under the GDPR to protect the confidentiality of those whose personal information is held.

- Employees of The Braunstone Foundation may not disclose any information about its customers / suppliers / volunteers / contacts or employees, including information as to whether or not any person is or has been an a customer’s / supplier / volunteer / contact or employee of The Braunstone Foundation unless they are clear that they have been given the authority to do so. Particular care should be taken in relation to any posting of personal information on the internet
- No employee of The Braunstone Foundation may provide references to prospective employers/ customers / suppliers / volunteers / contacts or employees, or others without the consent of the individual concerned. It is therefore essential that where The Braunstone Foundation is given as a referee the subject of their reference should be provided to The Braunstone Foundation with the necessary notification and consent.
- No employee may disclose personal data to the police or any other public authority unless that disclosure has been authorised by the Chief Officer, Head of Operations or Service Manager.

- Transfers

Personal data should not be transferred outside The Braunstone Foundation, and in particular not to a country outside the EEA

- except with the data subjects consent
- unless that country's data protection laws provide adequate levels of protection
- in consultation with the Chief Officer it is established that other derogations apply.

- Destruction of personal data

Personal data must not be held for longer than specified in relation to its collection and when such data has been earmarked for destruction, appropriate measures must be taken to ensure that the data cannot be reconstructed and processed by third parties.

- **Review**

This policy will be reviewed periodically to take account of changes in the law and guidance issued by the Information Commissioner.

- **Data Protection Contacts**

Angie Wright, Chief Officer or Linda Grubb, Head of Operations

The Braunstone Foundation  
Business Box  
3 Oswin Road  
Leicester  
LE3 1HR

- **Disciplinary Consequences of this Policy**

Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the European Economic Area) in contravention or breach of the Data Protection Act 1998 by anyone connected with or to The Braunstone Foundation will be treated seriously by The Braunstone Foundation and may lead to disciplinary action up to and including dismissal.



	<b>Computer records</b>	<b>Clerical records</b>
<p><b>Summary of all personal and sensitive data</b> This will provide you with list of all the data that we hold on you</p>		
<p><b>Summary of all case notes</b> This will provide you with a copy of all case notes we hold on you</p>		
<p><b>Other</b> Please list the names and addresses of the offices which may have your records. It would be helpful if you could also list the names / telephone or email addresses of staff you have dealt with.</p>		
<p><b>Other</b> Please be as specific as possible for example information relating to an appeal, grievance or complaint made.</p>		

**Any other information:**

---

### **Part C: Dates**

**What period you would like the personal information we send to you to cover?**

This applies to **clerical records only**. Computer records will contain **all** data held on the Braunstone Foundations computer systems at the time of your request.

The Braunstone Foundation does not hold personal information indefinitely. It may be that some information has been destroyed in line with our Data Retention policies.

<b>Personal information required for period</b>	from:	to:
---	-------	-----

---

### **Part D: Declaration**

**I declare that I have made a request for details of personal information held by the Braunstone Foundation as outlined above.**

**Signed:**

**Date**

:

**Please return this form to a Braunstone Foundation office or via email to:**

**Mail: [angie.wright@b-inspired.org.uk](mailto:angie.wright@b-inspired.org.uk) or to [linda.grubb@b-inspired.org.uk](mailto:linda.grubb@b-inspired.org.uk)**

**Address: Head Office, Business Box 3 Oswin Road. Leicester LE3 1HR or  
Neighbourhood Support team, 45 Wellinger Way. Braunstone, Leicester  
LE3 1RG**

## Request for personal information (Subject Access Request via a third party)

The Braunstone Foundation recognises that sometimes individuals agree to a third parties such as a solicitor, welfare rights organisation, government office or future employer seeking to obtain a copy of the personal information held by The Braunstone Foundation. However The Braunstone Foundation cannot disclose such information without lawful authority. The Braunstone Foundation takes the view that any consent to disclosure in these circumstances needs to be fully informed.

We have therefore developed a consent form which satisfies us that the individual is content for either all of some of the information to be realised to a third party. If you use this consent form in future applications for personal information, it will enable us to process applications without having to write to you for appropriate consent.

It is important that you complete as appropriate. The Braunstone Foundation may hold a large quantity of data about an individual and The Braunstone Foundation needs to ensure that we are providing only the information that is required.

### **Consent Form**

- Please arrange for this consent form to be completed and returned to The Braunstone Foundation whose address can be found at the end of this form.
- The Braunstone Foundation needs to ensure that we have identified the correct individual and have traced the correct records. If you do not provide this information we may need to contact you to obtain it which will delay the receipt of the personal information you require.
- Both declarations **MUST** be completed. The Braunstone Foundation will not accept any consent form which uses another form of words.
- In the case of the individual having a disability which prevents them from completing section E please ask them to make contact with The Braunstone Foundation directly who may be able to arrange assistance with the issues.



	<b>Computer records</b>	<b>Clerical records</b>
<p><b>Summary of all case notes</b> This will provide you with a copy of all case notes we hold on you</p>		
<p><b>Other</b> Please list the names and addresses of the offices which may have your records. It would be helpful if you could also list the names / telephone or email addresses of staff you have dealt with.</p>		
<p><b>Other</b> Please be as specific as possible for example information relating to an appeal, grievance or complaint made.</p>		

**Any other information:**

### Part C: Dates

**What period you would like the personal information we send to you to cover?**  
This applies to **clerical records only**. Computer records will contain **all** data held on the Braunstone Foundations computer systems at the time of your request.  
The Braunstone Foundation does not hold personal information indefinitely. It may be that some information has been destroyed in line with our Data Retention policies.

<b>Personal information required for period</b>	from:	to:
---	-------	-----

To meet its obligations under the Data Protection Bill, The Braunstone Foundation needs to be satisfied that the individual named in section A has given consent to the release of personal information to a third party.

### Part D: Declaration

**I declare that I have made a request for details of personal information held by the Braunstone Foundation as outlined above via a third party and that the person listed in section E is my authorised representative.**

**Signed:**

**Date**

:

---

### Part E – Consent

Insert the name of 3 <sup>rd</sup> party	
Insert the position of the person or their relationship to you	
Inset the organisation name represented by 3 <sup>rd</sup> party	
Insert the 3 <sup>rd</sup> parties address	

### Part E: Declaration

**I declare that I am authorised to request details of personal information held by the Braunstone Foundation for the person named in section A.**

**Signed:**

**Date**

**Please return this form to a Braunstone Foundation office or via email to:**

**Mail: [angie.wright@b-inspired.org.uk](mailto:angie.wright@b-inspired.org.uk) or to [linda.grubb@b-inspired.org.uk](mailto:linda.grubb@b-inspired.org.uk)**

**Address: Head Office, Business Box 3 Oswin Road. Leicester LE3 1HR or  
Neighbourhood Support team, 45 Wellinger Way. Braunstone, Leicester  
LE3 1RG**

