Impact Hub Bradford Data Protection Policy

1. Introduction

In the course of your employment with Impact Hub Bradford CIC, you are likely to collect, use, transfer or store personal information about employees, clients, customers and suppliers, for example their names and home addresses. The UK's data protection legislation, including the UK General Data Protection Regulations (GDPR) contains strict principles and legal conditions which must be followed before and during any processing of any personal information.

The purpose of this policy is to ensure that you are aware of your responsibility to comply with the principles and requirements of the data protection legislation, including the UK GDPR

It is mandatory that all employees, workers or contractors must read, understand and comply with the content of this policy and you must attend associated training relating to its content and operation. Failure to adhere to this policy is likely to be regarded as a serious disciplinary matter and will be dealt with under the Company's disciplinary rules and procedures.

2. Definitions

Data Subject: a living individual that the personal data relates to

Data Controller: the person or organisation that determines the means and the purpose of processing the personal data.

Data Protection Legislation: includes mainly the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), and the Privacy and Electronic Communications Regulation.

Data Processor: means a natural or legal person that processes personal data on behalf of the controller.

Personal data: is any information that identifies a living individual (data subject) either directly or indirectly.

Processing: is any activity relating to personal data, this includes collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.

Special categories of personal data: this includes any personal data which reveals a data subject's, ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.

Criminal offence data: is information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data Protection Principles

We are a data controller. This means that we are required by law to ensure that everyone who processes personal data and special categories of personal data during the course of their work with us does so in accordance with the data protection legislation, including the GDPR principles. In brief, the principles say that:

1. **PRINCIPLE 1: FAIRNESS, LAWFULNESS AND TRANSPARENCY**: Personal data must be processed in a lawful, fair and transparent way.
2. **PRINCIPLE 2: PURPOSE LIMITATION**: The purpose for which the personal information is collected must be specific, explicit and legitimate.
3. **PRINCIPLE 3: DATA MINIMISATION**: The collected personal data must be adequate and relevant to meet the identified purpose.
4. **PRINCIPLE 4: ACCURACY**: The information must be accurate and kept up to date.
5. **PRINCIPLE 5: STORAGE LIMITATION**: The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
6. **PRINCIPLE 6: DATA SECURITY**: The personal data must be kept confidential and secure and only processed by authorised personnel.
7. **PRINCIPLE 7: ACCOUNTABILITY**: requires you to take responsibility for what you do with personal data and how you comply with the other principles

IHB and all employees must comply with these principles and rules at all times in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

You must inform your line manager immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

4. What do the Principles mean in practice?

- **Fairness, Lawfulness and Transparency:** Personal data must be processed in a lawful, fair and transparent way.

Having an appropriate Privacy Notice that documents what personal data we collect and how we manage it, fulfils this requirement. The PN should detail accurate, transparent and clear details of the lawful and fair reason why we are processing the personal data. It must also explain how, when and for how long we propose to process the personal data for. this must be published in a way that is easily accessible to the individuals whose data we are processing.

- **Purpose limitation**: The purpose for which the personal information is collected must be specific, explicit and legitimate.

We must set out in the privacy notice how the personal data we collect will be used and what it will be used for. Specifying our purposes from the outset helps us to be accountable for our processing, and helps us avoid 'function creep'. It also helps individuals understand how we use their data, make decisions about whether they are happy to share their details, and assert their rights over data where appropriate.If our purpose for processing the data changes, the new purpose must be compatible with the original purpose, we get consent from the individuals, and it must be fair and lawful.

- **Data Minimisation**: The collected personal data must be adequate and relevant to meet the identified purpose.

You must only process personal data where you have been authorised to do so because it relates to your work or you have been delegated temporary responsibility to process the information. You must not collect, store or use unnecessary personal data and you must ensure that personal data is deleted, erased or removed in lin with the retention schedule and guidelines. You must not process or use personal data for non-work related purposes.

- **Accuracy**: Data must be kept accurate and up to date.

We must have processes in place that ensure all data subjects are able to update any changes in the information we hold about them. If in the course of your work, you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.

- **Storage Limitation**: Personal data must not be kept longer than it is needed, in a way that it will identify the individual it belongs to

IHB maintains a retention schedule that details how long the different categories of personal data we hold will be retained for, depending on legal, and operational requirements. Any data which the IHB decides it does not need to hold for a particular period of time will be destroyed in accordance with its retention of data policy.

- **Data Security**: Personal data must be kept confidential and secure at all times

To achieve this, IHB will commit to the follow steps:

A. To have in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. These procedures must always be adhered to and not overridden or ignored.

B. Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected from unintended destruction or change and is not seen by unauthorised persons.

C. Do not access another employee's records without authority as this will be treated as gross misconduct and it is also a criminal offence under the UK GDPR and Data Protection Act 2018.

D. Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.

E. Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager.

F. Ensure that when working on personal information as part of your job when away from your usual workplace, and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, particularly in matters of data security.

G. Ensure that hard copy personal information is disposed of securely, by shredding them, preferably, using the cross-shredding method so it is not easily put back together.

H. Manual personnel files and data subject files are confidential and are stored securely in a locker at our premises. Only authorised employees have access to these files. These will not be removed from their normal place of storage without good reason.

I. Any data stored on memory sticks, discs, portable hard drives or other removable storage media is kept securely with access restricted to a few named personnel.

J. Data held on computers are stored confidentially on Google drive.

K. The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed. For more information on other security measures in place at IHB, you can contact **hello.bradford@impacthub.net.**

5. Categories of information

At IHB, we may be required to process different categories of personal data about the individuals we engage with, to enable us perform our activities at the hub. These include the usual information that can identify an individual such as name, address, contact details, date of birth, gender, national insurance number, passport details, etc. To do this legally, we must have at least one legal basis in law from the applicable list in the next section below.

We may also collect other types of personal data known as special category data which are more sensitive and therefore, require more protection. These include information about an individual that relates to their health, race/ethnic origin, biometric data, religion/religious beliefs, political opinion, trade union membership, and sex life/sexual orientation. This category of information is special because it could create significant risk to the individuals and subject them to possible discrimination. This means that you should maintain a high level of security and you should only share this data with those who are also authorised to process that data. Article 9 of the UK GDPR prohibits the processing of any special category personal data unless we can show that we have a lawful basis to do so. We must show that we have an additional lawful basis under the Data Protection Act 2018.

All data should be processed in accordance with the privacy notice and at all times in a confidential manner.

6. Lawful basis

Under the UK GDPR, the lawful basis under which we process your personal data will be one or a more of the following:

a) **Consent**: you have given us consent to use and process your personal data for specific purposes.
b) **Contractual obligation**: we need the personal data to perform a contract with the individual, or to take steps towards performing a contract.
c) **Legal Obligation**: we need the personal data to comply with a statutory obligation.
d) **Legitimate Interest:** where the processing is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

You must always ensure that you keep a documentary inventory of the legal basis (or bases) which is being relied on in respect of each processing activity which you perform.

7. Transfer to another country

Transfer of personal data to countries or organisations outside of the UK should only take place if appropriate measures are in place to protect the security of that data.

IHB does not generally have a need to transfer data outside of the United Kingdom. We work with contractors and data processors that are located within the UK. However, if you are requested to share or transfer personal data to a country or organisation outside of the UK, it must be to a country that the UK has classed as having an adequate level of protection for processing of personal data. You must also ensure that IHB has in place safeguards to ensure this is done. You must speak to **Kamran Rashid at hello.bradford@impacthub.net** before you send personal data outside of the UK.

8. The data subjects rights

The data subject must be permitted to exercise their rights in relation to their personal data. Under the UK GDPR, these include:

- Right of access: Allow access to the personal data
- Right to rectification: Request corrections to be made to data
- Right to erasure (right to be forgotten) Request erasure of data
- Right to object to processing: Object to the processing of data
- Right to restriction: Request that processing restrictions be put in place
- Right to data portability: Request a transfer of personal data
- Right to complain to the supervisory authority (ICO)

There are different rules and timeframes that apply to each of these rights. You must follow our internal policies and procedures whenever you process or receive a request in relation to

any of the above rights. more information about the rights is available on the Information Commissioner's Office website here.

9. When will you need to seek consent?

In limited circumstances during your work you may need consent from a data subject in order to process personal data or special categories of data. You will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought.

However, in limited circumstances, you may find it necessary to request a data subject to provide written consent to allow the processing of special categories of personal data. You will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought. For example, in an employment context you should request the data subject's written consent to instruct a medical practitioner to prepare a medical report. If it becomes necessary to request consent to process special categories of personal data, you must provide the data subject with details of the information that will be required and why it is needed, so that they can make an informed decision as to whether they wish to provide consent.

You must not compel a data subject to provide written consent. Giving consent will always be a decision made by freewill and choice and is not a contractual condition. Consent can be withdrawn at any time without any reason provided. You must not subject a data subject to a sanction or detriment as a consequence of withdrawing consent. This would be viewed as a serious disciplinary issue.

10. Data Breach

What is a personal data breach?

A personal data breach is any security incident that has affected the confidentiality, integrity or availability (CIA) of personal data. A personal data breach will arise whenever any personal data is lost, destroyed, corrupted, accessed or shared without any proper authorisation. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

What to do in the event of a breach?

On becoming aware of an actual or potential breach, you should follow the internal breach reporting procedure or notify your line manager immediately. Remember, IHB has 72 hours under the UK GDPR, from when we became aware of the breach, to report it to the ICO, if it's a reportable breach. Therefore, it is essential that you report a breach as soon as you become aware of it so that it can be investigated accordingly. There is no consequence to you for reporting an actual or potential breach.

In the meantime, you can take the following immediate actions:

- Contain the breach;
- Assess the potential adverse consequences for individuals, based on how serious or

substantial these are, and how likely they are to happen; and

- To limit the scope of the breach by taking steps to mitigate the effects of the breach.

The person who is reporting the breach must provide as much information as possible to give a good understanding of the breach and help make a decision if it needs to be reported to the ICO.

Breach of the data protection legislation regulations can cause distress to the individuals affected by the breach and is likely to cause serious financial consequences or reputational damage to IHB.

11. Training

All employees that handle personal information must undergo data protection training at least on an annual basis. Employees with duties such as computer and internet security, marketing and database management may need specialist training to make them aware of particular data protection requirements in their work area.

IHB will provide employees with continuous training and updates on how to process personal data in a secure and confidential manner and in accordance with the spirit of the data protection legislation. Employees will be required to attend all training and to keep themselves informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

Employees must regularly review all data processing activities within their ownership and ensure that they are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

12. Sharing personal data

We may share personal data internally as is necessary. Employees must always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. Extra care and security must be taken when sharing special categories of data or transferring data outside of IHB to a third party.

If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from your line Manager in the first instance.

13. Direct Marketing

We are subject to specific rules under the UK GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing and we must ensure that data subjects are given this option at the first point of contact. When a data subject exercises their right to reject marketing you must desist immediately from sending further communications.

14. Changes to this policy

We reserve the right to change this policy at any time so please always check this document regularly to ensure you are following the correct procedures. All policies should be reviewed at least annually or when significant change occurs to the policy subject matter.

This policy was last updated in March 2024.The next Review date is March 2025.

Compliance with the UK GDPR is everyone's responsibility.

15. Version Control/History

Version No.	Author	Effective Date	Status/Comments (should include version status, i.e. draft or approved version)
0.1		March 2024	New policy
0.2			