The Blackford Centre

Data Protection Policy - Learner Guidance

Introduction

The Blackford Centre is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

This policy applies to all learners, who must comply with its terms.

This policy supplements our other policies relating to internet, email and privacy use. We may supplement or amend this policy by additional policies and guidelines from time to time.

This policy sets out how we seek to protect your personal data and ensure you understand the rules governing the use of personal data during the duration of a course.

What is personal data?

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'). Personal data includes:

- Your name.
- An identification number (e.g. National Insurance number).
- Location data.
- An online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion

- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

Fair and lawful processing

We will process your personal data fairly and lawfully in accordance with individuals' rights. This means that we will not process personal data unless you have consented to this happening.

In most cases where we process special categories of personal data we will require your *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law. We will clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

We ensure you are informed about the lawful basis for processing data, as well as the intended purpose. This is stated in our privacy notice.

Who is responsible for this policy?

As our data protection officer (DPO), Kit Sadgrove has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO at Support@inst.org for further information about this policy.

The principles

The Blackford Centre shall comply with the principles of data protection enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles.

The Principles are:
1. Lawful, fair and transparent
Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose
Data can only be collected for a specific purpose.

3. Data minimisation
Any data collected must be necessary and not excessive for its purpose.

4. Accurate
The data we hold must be accurate and kept up to date.

5. Retention
We cannot store data longer than necessary.

6. Integrity and confidentiality
The data we hold must be kept safe and secure.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless you have agreed to this or would otherwise reasonably expect this.

Choosing how we use your data

We understand that you trust us with your personal information and we are committed to ensuring you can manage the privacy and security of your personal information yourself. Please read our Privacy Policy for more information.

Third parties

If you enrol online, our system will send a copy of your email address to Trustpilot.com, who will invite you to provide independently verified feedback on our service. If you do not send a review Trustpilot will send you one (and only one) reminder seven days after the first email.

Trustpilot does not allow us to cancel or halt an invitation once it has received your email address. If you would prefer us not to send an email to Trustpilot, we recommend you enrol over the phone. This will allow us to stop the Trustpilot email.

How long do we keep your data for?

The Blackford Centre will not retain your personal information longer than necessary. We will hold on to the information you provide either while your account is in existence, or as needed to be able to provide services to you, or for as long as is necessary to provide support-related reporting and trend analysis only.

If legally required or if it is reasonably necessary to meet regulatory requirements, resolve disputes, prevent fraud and abuse, or enforce our Terms and Conditions, we may also retain some of your information for a limited period of time as required, even after you have closed your account or it is no longer needed to provide the services to you.

Storing data securely

We will ensure that all personal information supplied is held securely in accordance with the General Data Protection Regulation (EU) 2016/679, as adopted into law of the United Kingdom in the Data Protection Act 2018.

By providing telephone or email details, you consent to The Blackford Centre contacting you using that method. You have the right at any time to request a copy of the personal information we hold on you. This is called a subject access request. Should you want a copy of this, or would like to be removed from our database, please contact us at Support@inst.org

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure

How we deal with subject access requests

If you make a subject access request, we must provide you with a copy of the information requested, free of charge. This must occur without delay, and within one month of the request. We endeavour to provide you with access to your information in commonly used electronic formats, and where possible, provide you with direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but you will be informed within one month.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the learner specify the information they are requesting. This can only be done with express permission from the DPO.

What is the right to erasure?

Learners have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, we will contact and inform them of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

Rights of individuals

As a learner you have rights to your data which we must respect and comply with to the best of our ability. We must ensure you can exercise your rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay and no later than one month. This can be extended to two months with permission from the DPO.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making

- We must respect the rights of individuals in relation to automated decision making.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.
- We do not carry out profiling.