Introduction

The IBTC needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees, students and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures the IBTC:

- Complies with data protection law and follows good practice
- Protects the rights of staff, students, customers and partners
- Is open about how it stores and processes individuals' data.
- Ensure subjects rights are fully met.
- Protects itself from the risks of a data breach

Data Protection law

The Data Protection Act 1998 and forthcoming General Data Protection Regulation (GDPR) describes how organisations — including the IBTC— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act & (GDPR) is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held longer than absolutely necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy scope

This policy applies to:

- The head office of The IBTC
- All branches of The IBTC
- All staff, students and volunteers of The IBTC
- All contractors, suppliers and other people working on behalf of The IBTC

- It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 (GDPR). This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect The IBTC from some very real data security risks, including:

Breaches of confidentiality. For instance, information being given out inappropriately.
Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.
Unauthorised access to information For instance IT systems could be hacked or intruders could breach physical security and gain access to information.

Responsibilities

Everyone who works for or with IBTC has some responsibility for ensuring data is collected, stored and handled appropriately

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The **board of directors** is ultimately responsible for ensuring that the IBTC meets its legal obligations.

The basis of data protection

The data processed by the IBTC relates to information that is necessary for the company to discharge its duties under legislation and to ensure that the business operates effectively. Where data is collected or used for the purposes of marketing the subject's consent is actively sort. Essentially the subject MUST positively consent by indicating that they wish to be included in marketing initiatives and deciding which activities to participate in.
Where data relating to health or individual learning needs is collected it is necessary to enable the IBTC to discharges its duties under legislation eg The Health and Safety At Work

Act. Health and learning needs information will be shared with relevant staff only on a need to know basis.

Sharing of data

No data will be shared with third parties except where a legal obligation exists or to enable the IBTC to fulfil its obligations to specific government departments eg Revenue and Customs

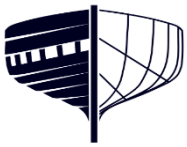
Subject rights

Under the DPA and the GDPR all those who are the subjects of data collected and processed by The IBTC have statutory rights. The IBTC fully acknowledges these rights and works to ensure they are met in full. The rights are as follows:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

If an individual contacts the company wishing to exercise these rights, it is called a subject access request.

Subject access requests from individuals should be made by email, telephone or letter addressed to the IBTC at info@ibtc.co.uk. Or at the company's postal address. The IBTC can



supply a standard request form, although individuals do not have to use this.

The IBTC will aim to provide the relevant data within 1 month.

The IBTC will always verify the identity of anyone making a subject access request before handing over any information.

General staff guidelines

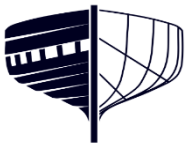
- The only people able to access data covered by this policy should be those who **need it for their work**.

- Data **should not be shared informally**. When access to confidential information is
- required, employees can request it from their line managers.

- **The IBTC will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

- These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.



- When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.
- These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.
- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices such as tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**
- Staff must only access data and the main network using their **personal credentials.**

Disclosing data for other reasons

In certain circumstances, the DPA and GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, The IBTC will disclose requested data. However, the IBTC will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

The IBTC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the company' website

Registered Office: IBTC Ltd. 6 Sea Lake Road, Oulton Broad, Lowestoft, Suffolk NR32 3LQ
Registered in England No. 5266445 Director: M Tupper VAT Registration No. 851 3253 45
Tel: 01502 569663 e-mail: info@ibtc.co.uk www.ibtc.co.uk