This document sets out the data protection policy of TCii Limited, trading as Terry Irwin. In this document, "Terry Irwin" means "TCii Limited, trading as Terry Irwin".

Terry Irwin needs to gather and use certain information about individuals. These can include clients, suppliers, business contacts, employees and other people with whom he has a relationship with or whom he may need to contact.

Terry Irwin is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of his legal obligations.

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

Key details

Policy prepared by:	Terry Irwin
Policy became operational on:	19 November 2021
Next review date:	19 May 2022

Why this policy exists

This data protection policy ensures that Terry Irwin:

- complies with data protection law and follows good practice
- protects the rights of staff, clients and partners
- is open about how he stores and processes individuals' data
- protects himself from the risks of a data breach.

Data protection law

The Data Protection Act 1998 describes how organisations – including TCii trading as Terry Irwin – 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 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 for any longer than necessary

(6) be processed in accordance with the rights of data subjects

(7) be protected in appropriate ways

(8) not be transferred outside the UK, unless that country or territory also ensures an adequate level of protection.

People, risks and responsibilities

Policy scope

This policy applies to:

- Terry Irwin
- all contractors, suppliers and other people working on behalf of Terry Irwin.

It applies to all data that Terry Irwin holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. 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 Terry Irwin 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 Terry Irwin uses data relating to them
- reputational damage – for instance, Terry Irwin could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Terry Irwin has some responsibility for ensuring that 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.

Key areas of responsibility

Terry Irwin is ultimately responsible for ensuring that he meets his legal obligations.

As **data protection officer**, Terry Irwin has overall responsibility for the day-to-day implementation of this policy and is responsible for:

- keeping all relevant parties updated about data protection responsibilities, risks and issues
- reviewing all data protection procedures and related policies, in line with an agreed schedule
- arranging data protection training and advice for the people covered by this policy
- answering questions on data protection from staff and anyone else covered by this policy
- dealing with requests from individuals to see the data Terry Irwin holds about them (also called “subject access requests”)
- checking and approving any contracts or agreements with third parties that may handle Terry Irwin’s sensitive data.

As **IT manager**, Terry Irwin is responsible for:

- ensuring that all systems, services, software and equipment used for storing data meet acceptable security standards

- performing regular checks and scans to ensure that security hardware and software is functioning properly
- evaluating any third-party services Terry Irwin is considering using to store or process data – for instance, cloud computing services.

As **marketing manager**, Terry Irwin is responsible for:

- approving any data protection statements attached to communications such as emails and letters
- addressing any data protection queries from clients, target audiences or media outlets
- where necessary, working with other staff to ensure that all marketing initiatives adhere to data protection laws and Terry Irwin's data protection policy.

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 Terry Irwin.
- Terry Irwin 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 internally 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 the data protection officer if they are unsure about any aspect of data protection.

Lawful basis for processing data

Terry Irwin must establish a lawful basis for processing data. At least one of the following conditions must apply whenever Terry Irwin processes personal data:

1. Consent

Terry Irwin holds recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. Contract

The processing is necessary to fulfil or prepare a contract for the individual.

3. Legal obligation

Terry Irwin has a legal obligation to process the data (excluding a contract).

4. Vital interests

Processing the data is necessary to protect a person's life or in a medical situation.

5. Public function

Processing the data is necessary to perform a task in the public interest or in the exercise of official authority, and the task or function has a clear basis in law.

6. Legitimate interest

The processing is necessary for Terry Irwin's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

In the case of Terry Irwin, in most cases the lawful basis will be either legitimate interest or consent. These provisions will apply to routine business data processing activities.

Special categories of personal data

Previously known as sensitive personal data, this means data about an individual that 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.

Terry Irwin does not hold or process any of these special categories of data.

Privacy policy

The Terry Irwin privacy policy, which can be found on the Terry Irwin website, states:

- the purposes for which Terry Irwin holds personal data on clients and employees
- the fact that Terry Irwin's work may require him to give information to third parties such as expert witnesses and other professional advisers
- the fact that clients have a right of access to the personal data Terry Irwin holds about them.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to Terry Irwin as IT and data protection officer.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it.

The following 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 – for example, 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. Terry Irwin encourages all staff to use a password manager to create and store their passwords.
- If data is stored on removable media (such as a CD, DVD or memory stick), 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 cloud computing services approved by the data protection officer.
- Servers containing personal data must 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 Terry Irwin's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices such as tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a strong firewall.

All possible technical measures must be put in place to keep data secure.

Data retention

Terry Irwin should retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons for which the personal data was obtained, but should be determined in a manner consistent with Terry Irwin's data retention guidelines.

Transferring data internationally

In accordance with the restrictions on international transfers, employees and other individuals covered by this policy must not transfer personal data anywhere outside the UK without first consulting the data protection officer.

Data use

Personal data is of no value to Terry Irwin unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. They should always access and update the central copy of any data.

Data accuracy and relevance

The law requires Terry Irwin to take reasonable steps to ensure data is kept accurate and up to date.

Terry Irwin will ensure that any personal data he processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. Terry Irwin will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that Terry Irwin correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the data protection officer.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure that data is updated – for instance, by confirming a client's details when they call.
- Terry Irwin will make it easy for data subjects to update the information he holds about them – for instance, via the Terry Irwin website.
- Data should be updated as and when inaccuracies are discovered. For instance, if a client can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure that marketing databases are checked against industry suppression files every six months.

Subject access requests

In accordance with the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. All individuals who are the subject of personal data held by Terry Irwin are entitled to:

- ask what information Terry Irwin holds about them and why
- ask how to gain access to it
- be informed of how to keep it up to date
- be informed of how Terry Irwin is meeting his data protection obligations.

If an individual contacts Terry Irwin requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at terry@terryirwin.com. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 14 days.

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

Disclosing data for other reasons

In certain circumstances, the Data Protection Act 1998 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Terry Irwin will disclose requested data. However, the data controller will check that the request is legitimate, seeking assistance from Terry Irwin's legal advisers where necessary.

Providing information

Terry Irwin 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, Terry Irwin has a privacy statement, which sets out how data relating to individuals is used by Terry Irwin. This statement is available on request, and is also available on the Terry Irwin website.

The General Data Protection Regulation (GDPR)

Where not specified previously in this policy, the following provisions will be in effect on or before 19 November 2021.

Privacy Notice – transparency of data protection

Being transparent and providing accessible information to individuals about how he will use their personal data is important for Terry Irwin. Below are details on how Terry Irwin collects data and what he will do with it.

What information is being collected?	Names, email addresses, IP addresses, company information and job titles, and, on a voluntary basis, other contact details such as telephone numbers and addresses
Who is collecting it?	Terry Irwin
How is it being collected?	Via registration forms for: Terry Irwin newsletters and/or other services; access to free downloadable articles on the Terry Irwin website; job applications
Why is it being collected?	To send communications such as newsletters and event invitations, and/or to enable individuals to access downloadable articles on the Terry Irwin website
How will it be used?	To manage mailing lists for the Terry Irwin newsletter, event invitations and occasional marketing communications
With whom will it be shared?	Terry Irwin employees and trusted subcontractors where necessary to provide requested services, and to third parties where necessary to comply with legal requirements **(see "Information sharing and disclosure" in the Terry Irwin privacy policy)**
Identity and contact details of any data controllers	Data protection officer: Terry Irwin – email terry@terryirwin.com
Details of transfers to third countries and safeguards	Information is not generally transferred outside the UK, and definitely not without consulting the data protection officer
Retention period	As long as is necessary for the provision of requested services such as sending of the Terry Irwin newsletter and/or enabling the downloading of articles or other material from the Terry Irwin website

Conditions for processing

Terry Irwin will ensure that any use of personal data is justified using at least one of the conditions for processing, and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Criminal record checks

Criminal record checks will only be carried out if and when justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

A data subject has the right to receive, upon request, a copy of their data in a structured format. Such requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The data protection officer will be responsible for conducting privacy impact assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the UK without a prior discussion with the data protection officer. Specific consent from the data subject must be obtained before their data is transferred outside the UK.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible, and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows Terry Irwin to:

- investigate the failure and take remedial steps if necessary
- maintain a register of compliance failures
- notify the supervisory authority of any compliance failures that are material, either in their own right or as part of a pattern of failures.

Monitoring

Everyone must observe this policy. The data protection officer has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

Terry Irwin takes compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under Terry Irwin's procedures, which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer.