Anti-Bribery & Anti-Corruption Policy 2020

October 2020

Printech Circuit Laboratories Ltd

Experienced at Different

Printech

Printech Circuit Laboratories Ltd

Anti-Bribery & Anti-Corruption Policy

❖ Policy Statement

'Printech Circuit Laboratories Ltd' is committed to conducting business in an ethical and honest manner, and is committed to implementing and enforcing systems that ensure bribery is prevented. The Company has zero-tolerance for bribery and corrupt activities. We are committed to acting professionally, fairly, and with integrity in all business dealings and relationships, wherever in the country we operate.

'Printech Circuit Laboratories Ltd' will constantly uphold all laws relating to anti-bribery and corruption in all the jurisdictions in which we operate. We are bound by the laws of the UK, including the Bribery Act 2010, in regards to our conduct both at home and abroad.

The Company recognises that bribery and corruption are punishable by up to ten years of imprisonment and a fine. If our company is discovered to have taken part in corrupt activities, we may be subjected to an unlimited fine, be excluded from tendering for public contracts, and face serious damage to our reputation. It is with this in mind that we commit to preventing bribery and corruption in our business, and take our legal responsibilities seriously.

❖ Scope

This policy applies to all employees (whether temporary, fixed-term, or permanent), consultants, contractors, trainees, seconded staff, home workers, casual workers, agency staff, volunteers, interns, agents, sponsors, or any other person or persons associated with us (including third parties), or any of our subsidiaries or their employees, no matter where they are located (within or outside of the UK). The policy also applies to Officers, Trustees, Board, and/or Committee members at any level.

In the context of this policy, third-party refers to any individual or organisation our company meets and works with. It refers to actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies – this includes their advisors, representatives and officials, politicians, and public parties.

Any arrangements our company makes with a third party is subject to clear contractual terms, including specific provisions that require the third party to comply with the Anti-Bribery Act 2010.

❖ Definition of Bribery

Bribery refers to the act of offering, giving, promising, asking, agreeing, receiving, accepting, or soliciting something of value or of an advantage so to induce or influence an action or decision.

A bribe refers to any inducement, reward, or object/item of value offered to another individual in order to gain commercial, contractual, regulatory, or personal advantage.

Bribery is not limited to the act of offering a bribe. If an individual is on the receiving end of a bribe and they accept it, they are also breaking the law.

Bribery is illegal. Employees must not engage in any form of bribery, whether it be directly, passively (as described above), or through a third party (such as an agent or distributor). They must not bribe a foreign public official anywhere in the world. They must not accept bribes in any degree and if they are uncertain about whether something is a bribe or a gift or act of hospitality, they must seek further advice from the company's compliance manager.

❖ What is and what is not acceptable?

This section of the policy refers to 4 areas:

- Gifts and hospitality.
- Facilitation payments.
- Political contributions.
- Charitable contributions.

Gifts and hospitality

'Printech Circuit Laboratories Ltd' accepts normal and appropriate gestures of hospitality and goodwill (whether given to/received from third parties) so long as the giving or receiving of gifts meets the following requirements:

a. It is not made with the intention of influencing the party to whom it is being given, to obtain or reward the retention of a business or a business advantage, or as an explicit or implicit exchange for favours or benefits.

b. It is not made with the suggestion that a return favour is expected.

c. It is in compliance with local law.

d. It is given in the name of the company, not in an individual's name.

e. It does not include cash or a cash equivalent (e.g. a voucher or gift certificate).

f. It is appropriate for the circumstances (e.g. giving small gifts around Christmas or as a small thank you to a company for helping with a large project upon completion).

g. It is of an appropriate type and value and given at an appropriate time, taking into account the reason for the gift.

h. It is given/received openly, not secretly.

i. It is not selectively given to a key, influential person, clearly with the intention of directly influencing them.

j. It is not above a certain excessive value, as pre-determined by the company's compliance manager (usually in excess of £100).

k. It is not offer to, or accepted from, a government official or representative or politician or political party, without the prior approval of the company's compliance manager.

Where it is inappropriate to decline the offer of a gift (i.e. when meeting with an individual of a certain religion/culture who may take offence), the gift may be accepted so long as it is declared to the compliance manager, who will assess the circumstances.

'Printech Circuit Laboratories Ltd' recognises that the practice of giving and receiving business gifts varies between countries, regions, cultures, and religions, so definitions of what is acceptable and not acceptable will inevitably differ for each.

As good practice, gifts given and received should always be disclosed to the compliance manager. Gifts from suppliers should always be disclosed.

The intention behind a gift being given/received should always be considered. If there is any uncertainty, the advice of the compliance manager should be sought.

Facilitation Payments and Kickbacks

'Printech Circuit Laboratories Ltd' does not accept and will not make any form of facilitation payments of any nature. We recognise that facilitation payments are a form of bribery that involves expediting or facilitating the performance of a public official for a routine governmental action. We recognise that they tend to be made by low level officials with the intention of securing or speeding up the performance of a certain duty or action.

The Company does not allow kickbacks to be made or accepted. We recognise that kickbacks are typically made in exchange for a business favour or advantage.

'Printech Circuit Laboratories Ltd' recognises that, despite our strict policy on facilitation payments and kickbacks, employees may face a situation where avoiding a facilitation payment or kickback may put their/their family's personal security at risk. Under these circumstances, the following steps must be taken:

a. Keep any amount to the minimum.

b. Ask for a receipt, detailing the amount and reason for the payment.

c. Create a record concerning the payment.

d. Report this incident to your line manager.

Political Contributions

'Printech Circuit Laboratories Ltd' will not make donations, whether in cash, kind, or by any other means, to support any political parties or candidates. We recognise this may be perceived as an attempt to gain an improper business advantage.

Charitable Contributions

'Printech Circuit Laboratories Ltd' accepts (and indeed encourages) the act of donating to charities – whether through services, knowledge, time, or direct financial contributions (cash or otherwise) – and agrees to disclose all charitable contributions it makes.

Employees must be careful to ensure that charitable contributions are not used to facilitate and conceal acts of bribery.

We will ensure that all charitable donations made are legal and ethical under local laws and practices, and that donations are not offered/made without the approval of the compliance manager.

❖ Employee Responsibilities

As an employee of 'Printech Circuit Laboratories Ltd', you must ensure that you read, understand, and comply with the information contained within this policy, and with any training or other anti-bribery and corruption information you are given.

All employees and those under our control are equally responsible for the prevention, detection, and reporting of bribery and other forms of corruption. They are required to avoid any activities that could lead to, or imply, a breach of this anti-bribery policy.

If you have reason to believe or suspect that an instance of bribery or corruption has occurred or will occur in the future that breaches this policy, you must notify the compliance manager.

If any employee breaches this policy, they will face disciplinary action and could face dismissal for gross misconduct.

A Managing Director has the right to terminate a contractual relationship with an employee if they breach this anti-bribery policy.

❖ Raising Concerns

This section of the policy covers 3 areas:

a. How to raise a concern.

b. What to do if you are a victim of bribery or corruption.

c. Protection.

How to raise a concern

If you suspect that there is an instance of bribery or corrupt activities occurring in relation to 'Printech Circuit Laboratories Ltd', you are encouraged to raise your concerns at as early a stage as possible. If you're uncertain about whether a certain action or behavior can be considered bribery or corruption, you should speak to your line manager, the compliance manager, the director, or the Head of Governance and Legal.

The Company will familiarise all employees with its whistleblowing procedures so employees can vocalise their concerns swiftly and confidentially.

What to do if you are a victim of bribery or corruption You must tell your compliance manager as soon as possible if you are offered a bribe by anyone, if you are asked to make one, if you suspect that you may be bribed or asked to make a bribe in the near future, or if you have reason to believe that you are a victim of another corrupt activity.

Protection If you refuse to accept or offer a bribe or you report a concern relating to potential act(s) of bribery or corruption, 'Printech Circuit Laboratories Ltd' understands that you may feel worried about potential repercussions. The Company will support anyone who raises concerns in good faith under this policy, even if investigation finds that they were mistaken.

'Printech Circuit Laboratories Ltd' will ensure that no one suffers any detrimental treatment as a result of refusing to accept or offer a bribe or other corrupt activities or because they reported a concern relating to potential act(s) of bribery or corruption.

Detrimental treatment refers to dismissal, disciplinary action, treats, or unfavourable treatment in relation to the concern the individual raised.

If you have reason to believe you've been subjected to unjust treatment as a result of a concern or refusal to accept a bribe, you should inform your line manager or the compliance manager immediately.

❖ Monitoring & Reviewing

'Printech Circuit Laboratories Ltd' compliance manager is responsible for monitoring the effectiveness of this policy and will review the implementation of it on a regular basis. They will assess its suitability, adequacy, and effectiveness.

Internal control systems and procedures designed to prevent bribery and corruption are subject to regular audits to ensure that they are effective in practice.

Any need for improvements will be applied as soon as possible. Employees are encouraged to offer their feedback on this policy if they have any suggestions for how it may be improved. Feedback of this nature should be addressed to the compliance manager.

This policy does not form part of an employee's contract of employment and 'Printech Circuit Laboratories Ltd' may amend it at any time so to improve its effectiveness at combatting bribery and corruption.

Brexit Statement 2020

October 2020

Printech Circuit Laboratories Ltd

Experienced at Different

Printech

Printech Circuit Laboratories Ltd

Brexit Statement

❖ Introduction

As you are aware, the UK officially left the EU on the 31st January 2020 and entered into a transition period during which we will continue to abide by the rules of the EU whilst negotiating a new trade agreement with our largest trading partner.

This transition period ends on the 31st of December 2020 and the UK Government have confirmed that there will be no extension to this, despite the current COVID-19 pandemic situation.

If a new deal cannot be agreed by the end of 2020, then from the 1st of January 2021, the UK and EU will revert to trading on WTO rules and the UK will essentially be a third-party country to the EU, as is the US and China for example.

If this 'NO DEAL' arrangement does come to fruition, then any goods arriving from the EU or leaving for the EU, will be subject to the normal customs processes already in place for our other third-party trading partners.

The UK Government have recently confirmed that the move to WTO rules and the imposing of import checks on goods from the EU, will be phased in during 2021 rather than full implementation from the 1st of January 2021. This will help UK businesses deal with the additional work involved with importing of goods, as well as ease delays at UK ports for a period.

❖ Printech Circuit Laboratories Ltd.'s Response

We continue to monitor the Brexit situation closely and remain prepared with measures to counteract the impact of these circumstances, ensuring a continued reliable supply of our products after 31st December 2020.

The key actions we have taken and are constantly reviewing are detailed below.

- Those materials imported from mainland Europe come via a well-established process with robust supply chains and we are working closely with our key suppliers to safeguard these supply chains to ensure continuous availability.

- We are encouraging our customers to review their stock levels and ensure orders are placed ahead of normal timing to protect against delays.
- We are continuing discussions with our Carriers to mitigate the risk of customs delays, including preparations for increase in customs administration.
- We are continuing to monitor the political landscape so we can effectively review the best way to mitigate the negative effects of Brexit.
- We are constantly updating our analysis of the financial impact of a no deal Brexit, including increased duty and tariffs, increased cost of freight and customs administration, foreign exchange fluctuations and are looking at ways to mitigate this to ensure minimal impact on our customers.
- We are also monitoring any travel issues for our employees during and after a no deal Brexit.

We recognise that many of our customers may have concerns. We would like to assure you that we are taking all reasonable steps to mitigate risk, where this is within our control. We will continue to review our position as more information is provided by the UK Government.
We encourage any of our customers to make contact with us if they have any direct concerns. We hope the measures outlined above gives you some reassurance that we have plans in place to mitigate any negative impact, as far as possible, but if you have any further queries, please do not hesitate to speak with your usual point of contact.

October 2020

Counterfeit & Fraudulent Product Policy 2019

December 2019

Printech Circuit Laboratories Ltd

Experienced at Different

Printech

Printech Circuit Laboratories Ltd

Counterfeit & Fraudulent Product Policy

❖ Overview

Printech Circuit Laboratories Ltd is aware of the potential risk and opportunity for immoral and unscrupulous suppliers to supply products, components, parts, chemicals and other materials that are classified as counterfeit to Printech Circuit Laboratories Ltd. Counterfeit product has become a growing concern in customers' supply chains as customers or distributors secure lower cost alternative sources. This policy outlines our companies' approach to ensuring no counterfeit, inferior, fake or bogus parts, components and materials are purchased or used in the manufacture and supply of our products.

❖ Commitment

Printech Circuit Laboratories Ltd commits to protecting brand equity through preventing any counterfeit and fraudulent products and parts, including low quality and grade parts, from entering into our supply chain through strict avoidance, mitigation, monitoring and verification process.

❖ Our Policy

- Printech Circuit Laboratories Ltd will work tirelessly to ensure all goods and services shall only be purchased or procured through known and reputable sources from UK, European and International manufacturers/suppliers or their authorized distributors. Suppliers will be asked to warrant their products as per company requirements.
- Printech Circuit Laboratories Ltd do not purchase refurbished supplies/products for manufacturing.
- All suppliers shall be subject to quality-based monitoring and evaluation.
- In cases of suspected counterfeit or fraudulent parts found at Goods Inward, the parts shall be quarantined immediately. The supplier will be informed together with reasons and evidence, if available. If the issue cannot be resolved within a short period of time, or will result in a delay in delivery, then our customer will be informed. Quality procedures allow for advising the customer of any concerns and for forwarding parts, pictures and any other evidence for their opinion.
- Suppliers are obliged and encouraged to offer every assistance to the authorities in the event of counterfeit products being discovered. They may also be asked to prove due diligence.
- Any supplier who is subject to two issues of counterfeit or inferior goods delivery within a 12-month period will be automatically removed from the approved supplier list.

❖ Identification of Counterfeit Goods

- **Product Condition**
  Resurfaced/refinished evidence of re-work, wrong colouring, shape or size, evidence of previous use.
- **Lot Information**
  Unusual serialization or reference numbers, lot information missing.
- **Paperwork**
  Accompanying paperwork has poor spelling and/or grammar, errors or evidence of tampering, missing information or does not relate to the delivered product.
- **Unusual Location**
  Items delivered from a location differing from previous or prohibited locations.
- **Low Price**
  A price significantly lower than historical pricing data or market norms.
- **Availability**
  Obsolete or scarce supplies suddenly becoming available.
- **Unfamiliar Supplier**
  Supplier or agent/stockist not known or previously used.

18 December 2019

Data Protection Policy

2023

February 2023

Printech Circuit Laboratories Ltd

Experienced at Different

Printech

Printech Circuit Laboratories Ltd

CONTENTS

1. Interpretation 3

2. Introduction 4

3. Scope 5

4. Personal data protection principles 6

5. Lawfulness & Fairness.....7

6. Consent 7

7. Transparency (notifying Data Subjects) 8

8. Purpose limitation 8

9. Data minimisation 9

10. Accuracy 9

11. Storage limitation 9

12. Security integrity and confidentiality 10

13. Reporting a Personal Data Breach 11

14. Transfer limitation 11

15. Data Subject's rights and requests 11

16. Accountability 12

17. Record keeping 12

18.Direct marketing.....13

19. Sharing Personal Data 13

20. Changes to this Data Protection Policy 13

21. Employment Records.....14

1. Interpretation

Definitions:

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name: Printech Circuit Laboratories Limited.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Officer (DPO): the person or department required to be appointed in specific circumstances under the UK GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Guidelines: The Company privacy and UK GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2. Introduction

This Data Protection Policy sets out how Printech Circuit Laboratories Limited ("we", "our", "us", "the Company") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers,

customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf. This Data Protection Policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, or otherwise then you must comply with the Related Policies and Privacy Guidelines.

This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

All managers are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. The post is held by the Administration Department.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see paragraph 5);

b) if you need to rely on Consent and/or need to capture Explicit Consent (see paragraph 6);

c) if you need to draft Privacy Notices (see paragraph 7);

d) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 11);

e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 12);

f) if there has been a Personal Data Breach (paragraph 13);

g) if you are unsure on what basis to transfer Personal Data outside the UK (see paragraph 14);

h) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 15);

i) whenever you are engaging in a significant new, or change in, Processing activity or plan to use Personal Data for purposes other than what it was collected for;

j) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 18); or

k) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 19).

4. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

a) Processed lawfully, fairly and in a transparent manner (Lawfulness & Fairness);

b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

d) accurate and where necessary kept up to date (Accuracy);

e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Lawfulness & Fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The UK GDPR allows Processing for specific purposes, some of which are set out below:

a) the Data Subject has given his or her Consent;

b) the Processing is necessary for the performance of a contract with the Data Subject;

c) to meet our legal compliance obligations;

d) to protect the Data Subject's vital interests;

e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices;

6. Consent

A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

When processing Special Category Data or Criminal Convictions Data (which may include, but are not limited to, Basic/Enhanced DBS and NSVS checks), we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that the Company can demonstrate compliance with Consent requirements.

7. Transparency (notifying Data Subjects)

The UK GDPR requires Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis, which contemplates our proposed Processing of that Personal Data.

If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

You must comply with the Company's guidelines on drafting Privacy Notices.

8. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

9. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

10. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time. You must comply with the Company's guidelines on Data Retention.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records

retention schedules and policies. This includes requiring third parties to delete that data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

12. Security integrity and confidentiality

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and

c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

13. Reporting a Personal Data Breach

The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

14. Transfer limitation

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the UK if one of the following conditions applies:

a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

b) appropriate safeguards are in place such as standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism;

c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

You must comply with the Company's guidelines on cross-border data transfers.

15. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time;

b) receive certain information about the Controller's Processing activities;

c) request access to their Personal Data that we hold;

d) prevent our use of their Personal Data for direct marketing purposes;

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

f) restrict Processing in specific circumstances;

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

i) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

k) make a complaint to the supervisory authority;

l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format;

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the Administration Department and comply with the company's Data Subject response process.

16. Accountability

The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.
The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy.

17. Record keeping

The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

18. Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

You must comply with the Company's guidelines on direct marketing to customers.

19. Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless consent has been acknowledged.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You must comply with the Company's guidelines on sharing data with third parties.

20. Changes to this Data Protection Policy

We keep this Data Protection Policy under regular review.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

21. Employment Records

ABOUT THESE GUIDELINES

These guidelines support Printech Circuit Laboratories Limited's Data Protection Policy and adopt its definitions.

The guidelines are intended to ensure that 'Printech Circuit Laboratories Limited' processes personal data in the form of employment records in accordance with the personal data protection principles, in particular that:

- Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When personal data is no longer needed for specified purposes, it is deleted or anonymised as provided by these guidelines.

- Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

- Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

- Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The Data Protection Officer (DPO) is responsible for overseeing these guidelines. Any questions about the operation of the guidelines should be submitted to the DPO.

LOCATION OF EMPLOYMENT RECORDS

Printech Circuit Laboratories Limited's Administration Department holds employment records and can be contacted with any enquiries relating to your personal data.

KEEPING INFORMATION UP TO DATE

Printech Circuit Laboratories Limited needs to ensure that your personal details are up to date and accurate.

When you first start working for Printech Circuit Laboratories Limited we record your name, address, next of kin, and contact telephone details. In the event that any of these details change you should inform the Administration Department. You are expected to update personal information on a regular basis or whenever necessary.

GENERAL PRINCIPLES ON RETENTION AND ERASURE

Printech Circuit Laboratories Limited's approach to retaining employment records is to ensure that it complies with the data protection principles referred to in these guidelines and, in particular, to ensure that:

- Employment records are regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary to facilitate you working for Printech Circuit Laboratories Limited.

- Employment records are kept secure and are protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Where appropriate Printech Circuit Laboratories Limited uses anonymization to prevent identification of individuals.

- When records are destroyed, whether held as paper records or in electronic format, Printech Circuit Laboratories Limited will ensure that they are safely and permanently erased.

RETENTION AND ERASURE OF RECRUITMENT DOCUMENTS

Printech Circuit Laboratories Limited's expects to keep candidate’s personal information for six months from the communication of the outcome of the recruitment exercise which takes account of both the time limit to bring claims and for claims to be received by Printech Circuit Laboratories Limited.

Information relating to successful candidates will be transferred to their employment record with Printech Circuit Laboratories Limited. This will be limited to that information necessary for the working relationship and, where applicable, that required by law.

Following a recruitment exercise information, in both paper and electronic form, will be held by the Administration Department. Destruction of that information will take place in accordance with these guidelines.

RETENTION AND ERASURE OF EMPLOYMENT RECORDS

Printech Circuit Laboratories Limited has regard to recommended retention periods for particular employment records set out in legislation, referred to in the table below. However, it also has regard to legal risk and may keep records for up to seven years (and in some instances longer) after your employment or work with us has ended.

Type of employment record	Retention period
Recruitment records may include: Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) Criminal records checks. (These may be transferred to a successful candidate's employment file as they are relevant to the ongoing relationship.)	Six months after notifying candidates of the outcome of the recruitment exercise.
Criminal Convictions Data/Checks These may include: Basic/Enhanced Disclosure Barring Service National Security Vetting Solution (These will be updated as necessary as they are relevant to the ongoing relationship.)	In accordance with guidance from the issuing body.
Immigration Data/Checks	Three years after the termination of employment.
Contracts These may include: Written particulars of employment. Contracts of employment or other contracts. Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.

Collective agreements Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for seven years after employment ends.
Payroll and wage records Payroll and wage records Details on overtime. Bonuses. Expenses. Benefits in kind.	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.

Record of advances and loans to employees	While employment continues and for seven years after employment ends.
Personnel records These include: Qualifications/references. Consents for the processing of special categories of personal data. Annual leave records. Annual assessment reports. Disciplinary procedures. Grievance procedures. Death benefit nomination and revocation forms. Resignation, termination and retirement.	While employment continues and for seven years after employment ends.
Records in connection with working time Working time opt-out	Three years from the date on which they were entered into.
Records to show compliance, including: Time sheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.
Maternity records These include: Maternity payments. Dates of maternity leave. Period without maternity payment. Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends.
Accident records These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.

(GDPR) General Data Protection Regulation Compliance 2018

May 2018

Printech Circuit Laboratories Ltd

Experienced at Different

Printech

Printech Circuit Laboratories Ltd

(GDPR) General Data Protection Regulation Policy

❖ Data Protection Laws

In this Policy, the 'Data Protection Laws' means the General Data Protection Regulation (the GDPR) together with all other applicable legislation relating to privacy or data protection in force from time to time. You should share this Policy with your employees and colleagues where you have provided us with personal information about them (and where it is reasonable to do so).

❖ Controller & Processor

As defined by the GDPR, a Controller means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data.
A Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
Printech Circuit Laboratories Ltd is Controller for the purposes of the Data Protection Laws.
This Policy explains how Printech Circuit Laboratories uses and protects the personal information that they hold about you. Printech Circuit Laboratories Ltd is registered with the Information Commissioner's Office (ICO) registration number z6797100. Contact details for Printech Circuit Laboratories Ltd are set out at the end of this Policy.

❖ What is personal information?

Personal information broadly means information that identifies (or which could, with other information that we hold or are likely to hold) a living individual. This includes any information provided to us by or on behalf of you.

What types of personal information about you might we hold?
We collect and process the information about you that you provide:

- To carry out our obligations arising from any agreement that we have with, or concerning, you and to provide you with the information and services that you request from us.
- To notify you about services provided and any changes to those services.
- For statistical, accounting and reference purposes.
- For internal record keeping.
- For risk management purposes.
- Complying with our legal obligations, any relevant industry or professional rules and regulations.

- Complying with demands or requests made by any relevant regulators, government departments and law enforcement or tax authorities or in connection with any disputes or litigation.
- In connection with any sale, merger, acquisition, disposal, reorganisation or similar change of Printech Circuit Laboratories Ltd business.

In addition, Printech Circuit Laboratories Ltd may use your information:

- To enable our sub-contractors to provide aspects of our services to you.
- To analyse and improve the services we provide.
- To allow you to share content and materials on our website via social media or other communication means.
- To give you information on products and services which you have asked for or which we think may be of interest to you.

❖ How long do we keep your information for?

We will hold your personal information on our systems for as long as is necessary for Printech Circuit Laboratories Ltd to provide goods and service to you.
So, for example, if your required goods/service is ongoing, we will hold your information until the transaction is complete.
We will hold your information indefinitely, if you are a repeat customer, in case there are any further goods/services we can provide you.

❖ Who do we share the information with?

Printech Circuit Laboratories Ltd do not provide customer information to third parties with the exception of relevant regulators, government departments and law enforcement or tax authorities or in connection with any disputes or litigation.

❖ Security

We will use strict procedures and security features to safeguard against the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
All our employees are obliged to respect the confidentiality of such data provided to us and as required under applicable data protection or other legislation.

❖ Policy Changes

We keep this Policy under review and may change it at any time.

25 May 2018

Human Rights & Labour Standards Policy 2019

December 2019

Printech Circuit Laboratories Ltd

Experienced at Different

Printech

Printech Circuit Laboratories Ltd

Human Rights & Labour Standards Policy

❖ Introduction

The principles and guidelines set out in the Policy are derived from the United Nations Universal Declaration of Human Rights, the International Labour Organisation's Declaration on Fundamental Principles and Rights at Work, and reflects our aim of respecting human rights as laid out in the Human Rights Act 1998, and the United Nations Guiding Principles on Business and Human Rights.
The underlying Policy applies to all Printech Circuit Laboratories Ltd directors, officers and employees.

❖ Policy Statement

Printech Circuit Laboratories Ltd seeks to provide a work environment where employees are treated with respect, dignity and consideration. This commitment is built up on a framework of policies and procedures designed to ensure fairness in the recruitment, development and retention of employees.

❖ General Principles

- All employment must be in compliance with all applicable laws and regulations of the countries in which Printech Circuit Laboratories Ltd operates. Where the applicable local laws and regulations require higher or additional levels of protection of human and employment rights than those on this policy, the local laws and regulations will take precedence.
- All Printech Circuit Laboratories Ltd employees are required to report any actual, suspected or potential violations of all Company Policies, including the Human Rights and Labour Standards Policy. Failure to do so may lead to disciplinary action, up to and including termination of employment.
- This Policy shall be reviewed on an annual basis and updated where necessary to ensure the continuous preservation of working conditions and management of labour risks in Printech Circuit Laboratories Ltd operations.
- Printech Circuit Laboratories Ltd shall utilize sufficient resources to give effect to its commitment to year-on-year protection to working conditions and labour risks in its operations.

❖ Specific Provisions

- **Human Rights**
  Printech Circuit Laboratories Ltd supports and complies with the United Nations Universal Declaration of Human Rights and seeks to honour the principles of internationally recognized human rights wherever it operates. Each employee shall be treated with dignity and shall not suffer harassment, physical or mental punishment and other forms of abuse.
  Printech Circuit Laboratories Ltd have transparent and effective grievance mechanisms to enable the remediation of adverse human rights impacts that may arise in its operation, and effective employee engagement which welcomes feedback from employees on all matters of business.

- **Compulsory Labour and Human Trafficking**
  Printech Circuit Laboratories Ltd does not accept, nor condone, any form of modern slavery whether forced, compulsory or trafficked labour. Without limitation, Printech Circuit Laboratories Ltd does not engage in sweatshop labour, convict labour or indentured labour under penal sanction.
  All employees shall provide their services to the Company on an entirely voluntary basis and no-one shall be forced to remain in the employ of Printech Circuit Laboratories Ltd against their will.
  Printech Circuit Laboratories has a zero-tolerance approach to modern slavery and encourages employees to raise concerns about issue or suspicion of modern slavery in any part of the Printech Circuit Laboratories Ltd business at the earliest opportunity.
- **Child Labour**
  Printech Circuit Laboratories Ltd adheres to and strictly complies with international child labour conventions and child labour laws and regulations in the countries in which it operates.
  The minimum age of a Printech Circuit Laboratories Ltd employee shall be not less than the age of completion of compulsory education, and in any event, shall not be less than 16 years.
  Where the work concerned is by nature, or the circumstances in which it is carried out, deemed to be “hazardous”, the minimum age of the Printech Circuit Laboratories Ltd employee shall not be less than 18 years.
- **Discrimination**
  Printech Circuit Laboratories Ltd strictly prohibits discrimination and harassment against any employee or applicant for employment, whether such discrimination or harassment is based on sex, race, age, colour, ancestry, religion, belief, disability, sexual orientation, marital status or any other feature protected by law.

18 December 2019

Conflict of Interest Policy & Procedure 2020

October 2020

Printech Circuit Laboratories Ltd

Experienced at Different

Printech

Printech Circuit Laboratories Ltd

Conflict of Interest Policy & Procedure

❖ Brief

'Printech Circuit Laboratories Ltd' Conflict of Interest Policy refers to any case where an employee's personal interest might contradict the interest of the company they work for. This is an unwanted circumstance as it may have heavy implications on the employee's judgement and commitment to the company, and by extension to the realization of its goals. This policy will outline the rules regarding conflict of interest and the responsibilities of employees and the company in resolving any such discrepancies.

❖ Scope

'Printech Circuit Laboratories Ltd' Conflict of Interest Policy applies to all prospective or current employees of the company, as well as independent contractors and persons acting on behalf of the company.

❖ Elements

The relationship of 'Printech Circuit Laboratories Ltd' with its employees should be based on mutual trust. As the company is committed to preserve the interests of people under its employment, it expects them to act only towards its own fundamental interests.

Conflict of interest may occur whenever an employee's interest in a particular subject may lead them to actions, activities or relationships that undermine the company and may place it to disadvantage.

❖ What is an employee conflict of interest?

This situation may take many different forms that include, but are not limited to, conflict of interest examples:

- Employees' ability to use their position with the company to their personal advantage
- Employees engaging in activities that will bring direct or indirect profit to a competitor
- Employees owning shares of a competitor's stock
- Employees using connections obtained through the company for their own private purposes
- Employees using company equipment or means to support an external business
- Employees acting in ways that may compromise the company's legality (e.g. taking bribes or bribing representatives of legal authorities)

The possibility that a conflict of interest may occur can be addressed and resolved before any actual damage is done. Therefore, when an employee understands or suspects that a conflict of interest exists, they should bring this matter to the attention of management so corrective actions may be taken. Supervisors must also keep an eye on potential conflict of interests of their subordinates.

The responsibility of resolving a conflict of interest starts from the immediate supervisor and may reach senior management. All conflicts of interest will be resolved as fairly as possible. Senior management has the responsibility of the final decision when a solution cannot be found.

In general, employees are advised to refrain from letting personal and/or financial interests and external activities come into opposition with the company's fundamental interests.

Note: *The same principles apply to the company in regards to its clients. When applicable, we are committed to not offer services or form partnerships with companies who are in direct competition with one of our existing clients.*

❖ Disciplinary Consequences

In cases when a conflict of interest is deliberately concealed or when a solution cannot be found, disciplinary action may be invoked up to and including termination.