SPD Business Conduct Manual

August 2022

Contents

Letter from the CEO

Dear Colleagues

The success of SPD and our flagship Clearblue brand has been founded over more than 35 years on our ability to match great technical innovation with an in depth understanding of the needs of our consumers. But just as important in our success, has been the reputation that we have built over this time for reliability, integrity and ethical business conduct.

Our future success depends on maintaining this reputation and acting with integrity in all our business dealings. This can only be achieved if we all act with the highest ethical standards when engaged in any business activity.

The SPD Business Conduct Manual and the policies referenced within it provide a framework and guidance for all SPD people to follow in their every day work. I urge you to read it and follow the principles within it, both in letter and in spirit and always speak up if you feel that things are being done that are in conflict with those principles.

I truly believe that long term success is founded on sticking to our core values and principles and by doing so, we will continue to build on our success in the future.

Joanne Scaife
CEO

Introduction

SPD Swiss Precision Diagnostics GmbH and its subsidiary SPD Development Company Limited (referred to collectively as “SPD” in this Manual) operate in a complex and highly regulated industry and across numerous international borders.

As a result, when conducting business, SPD is subject to, and must comply with, many different international standards, regulations and laws.

In today’s business world there is now ever increasing scrutiny and pressure coming from consumers, shareholders, regulators, governments and international institutions, for businesses to be seen as good citizens, acting in the long-term interests of society rather than merely pursuing short-term profit motives.

SPD is an international business that trades on the quality and performance of its products, on the loyalty and trust of its consumers – built over many years and invested in the Clearblue brand and on its reputation as a technology leader and innovator in the fields of women’s health and in vitro diagnostics.

To protect this hard won reputation, we must therefore always aspire to the highest standards of business conduct and behaviour, so that we can continue to enjoy the trust of our consumers in the Clearblue brand, the confidence and respect of our business customers, partners and external regulators and the commitment and pride of our employees.

The purpose of the SPD Business Conduct Manual is to set out the core ethical and legal principles that underpin the way in which SPD does business in order to achieve these aims.

These principles apply to all employees, directors, contractors and consultants and in some instances to suppliers of SPD.

The SPD Business Conduct Manual is split into three sections

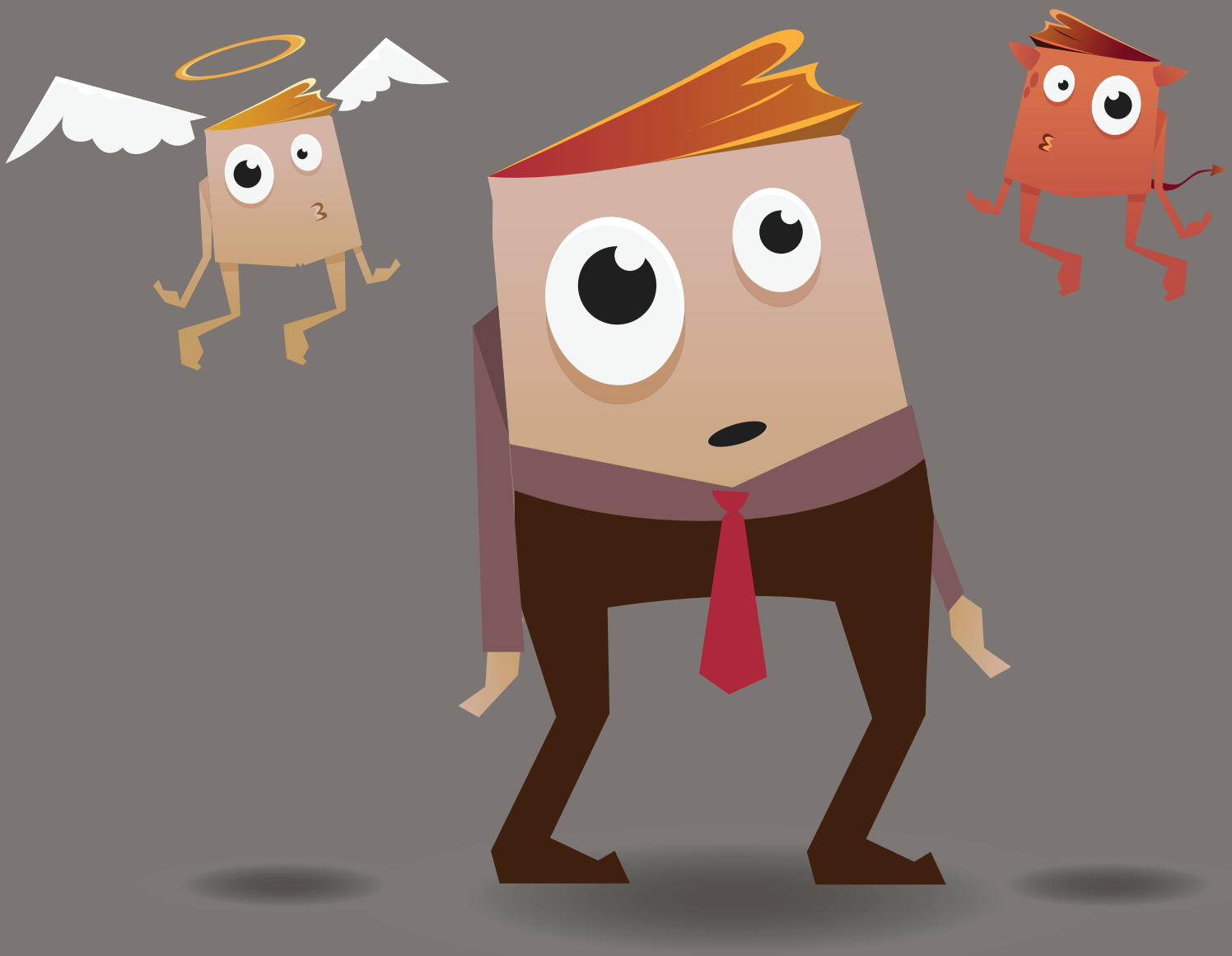
Section 1 : What SPD Expects of You

Section 2 : Expectations of SPD in the Workplace

Section 3 : How SPD Complies with Statutes and Regulations

In many cases additional supporting information may be found within specifically documented SPD policies and procedures. You are encouraged to consult these documents for further information.

1



What SPD Expects of You

1.1

Personal Behaviour

Ethical business conduct begins and ends with the standards of personal and professional behaviour displayed by our employees, directors, contractors and consultants.

Therefore, as a minimum SPD expects that you will:

- Comply with the law in all countries where you operate and avoid actions that discredit either you or SPD.
- Comply with all applicable SPD business processes, policies and internal control systems.
- Treat people, with courtesy, dignity and respect and avoid violent or intimidating behaviour.
- Act with honesty and integrity. Do not allow bias or undue influence from others to override your professional judgment.
- Avoid actions or relationships that might conflict or appear to conflict with your job responsibilities or the interests of SPD. If you believe such a conflict of interest exists, you must disclose it to SPD.
- Protect SPD's physical assets, intellectual property and all company confidential data.
- Do not disclose any such information or property to third parties without proper and specific authority (unless there is a legal or professional right or duty to disclose), nor use the information for personal advantage.
- Maintain your professional competence and act diligently in accordance with applicable technical and professional standards.
- Act with a duty of care for the safety of yourself and others. Do not place yourself or those you work with at unreasonable risk when conducting your business activities.

If in doubt, let your common sense guide you. It may help if you ask yourself the following questions:

- Does my action conform with SPD's minimum expected standards of behaviour (listed above)?
- Is my action consistent with approved SPD policies and processes?
- Could my action appear improper in a legal or ethical context?
- Could my action bring discredit to me or SPD if disclosed?
- Can I defend my action to my manager, other colleagues and to the public?
- Does my action meet my personal code of behaviour?

Anyone found to be acting in violation of these behavioural standards may be subject to disciplinary action, potentially resulting in termination of employment.

For more information please refer to the Employee Code of Conduct (POLICY-0068).

1.2

Raising Concerns of Wrongdoing

All organisations face the risk of things going wrong from time to time, or of unknowingly harbouring illegal or unethical conduct.

A culture of openness and accountability is essential in order to prevent such situations occurring and to address them when they do occur.

Therefore SPD encourages the reporting of suspected fraud, misconduct or wrongdoing by any individual or group of individuals as soon as possible, in the knowledge that:

- Your concerns will be taken seriously and investigated thoroughly, promptly and confidentially,
- You will be able to raise genuine concerns without fear of reprisals or victimisation, even if you turn out to be mistaken, and
- Your continued employment and opportunities for future promotion or training within SPD will not be prejudiced because you have raised a legitimate concern.

You should raise your concerns if you have a reasonable belief – you do not need proof that any of the following is being, has been, or is likely to have occurred:

- A criminal offence, e.g. fraud, bribery (including making a gift or a payment to any person to influence this person to perform in breach of their duties e.g. a government official, a government employee, a private person, an employee of a company, etc.)
- A miscarriage of justice
- An act creating risk to health and safety
- An act causing damage to the environment
- A breach of any other legal obligation, e.g. data protection, the Employee Code of Conduct, general compliance
- Concealment of any of the above

You can raise a concern with your manager, a member of the HR Team or with SPD Legal.

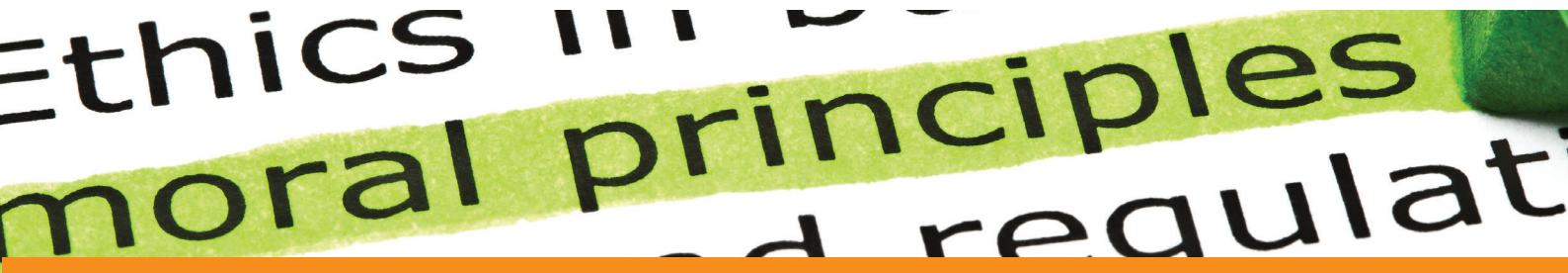
If for any reason you want to raise concerns of wrongdoing anonymously you can ring the Whistleblowing Hotline on:

•0800 047 4037 (from the UK)

•+44 0161 836 9499 (from outside the UK)

The hotline is managed by an external party, who will pass on your report anonymously to both the Managing Director, based in Bedford and the General Counsel and Chief Compliance Officer, based in Geneva, for further investigation.

For more information please refer to the Whistleblowing Policy (POLICY-0069).



1.3

Acceptable Use of Information Technology (IT) Tools

SPD provides its employees and contractors with a variety of information technology (IT) tools to assist them in carrying out their work. However, misuse or abuse of these tools can lead to reduced productivity, wasted company resources, legal liability for the company and/or individual employees, and ultimately, impaired business performance.

The following statements are intended to set out the framework under which all SPD employees and contractors using business IT tools can ensure that they are doing the right thing.

- The primary use of company-owned hardware and software must be for SPD business purposes. Personal use of company owned devices should be done in a manner that is consistent with the other sections of this Policy.

The following activities are prohibited

- installation or distribution of “pirated” or other software products that are not appropriately licensed.
- unauthorised copying of copyrighted material.
- revealing account passcodes to other users.
- using a company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
- providing information about, or lists of the Organisation’s users/customers to external parties.
- any form of harassment via email or telephone.
- unauthorised use, or forging, of email header information.
- creating or forwarding “chain letters” or other such schemes of any type.
- setting up automatic forwarding of e-mails to external addresses.
- placing any of the Organisation’s material on a publicly accessible internet site without prior approval.
- procurement and installation of hardware and software for personal use - including games, file sharing programs, instant messaging applications and social networking products (unless otherwise authorised).

In order to ensure system integrity and security, as well as application performance, network and system usage is passively monitored by our IT service providers Abbott Rapid Diagnostics Information Technology (ARDx IT) and Procter & Gamble (P&G).

SPD may obtain access to an individual’s IT system usage records if there is a legitimate and specific reason e.g. if a concern has been raised about inappropriate use which is potentially not acceptable use (as described in this Policy), or if SPD is legally required or subpoenaed to do so.

Anyone found to be acting in violation of SPD’s IT usage policy may be subject to disciplinary action, potentially resulting in termination of employment.

For more information please refer to the Information Technology Usage and Information Security Policy (POLICY-0067).

1.4

Information Security

It is your responsibility to ensure that you take all reasonable measures to protect and keep secure any business confidential data, intellectual property or other business sensitive information that comes into your possession.

Any such information must only be disclosed to the following:

- Fellow SPD employees with a legitimate need to know
- Third parties only under a non disclosure agreement and in the furtherance of SPD business objectives
- If there is a legal requirement to disclose the information

General precautions that should be taken to protect SPD business information include the following:-

- attending and putting into practice what is learned during staff awareness training
- locking your device when not in use
- ensuring Two Factor Authentication (2FA) is enabled on any system that requires and supports it
- not disclosing passwords or 2FA codes
- using Standard User accounts on devices rather than one with Administrator privileges (unless Admin privileges are explicitly granted by ARDx or P&G Information Security teams).
- use of strong passwords containing random alphanumeric (A, B, C, 1, 2, 3) and non-alpha numeric (#!?/), upper/ lower case characters, or word sequences.
- not disclosing any sensitive information when using devices in front of customers, suppliers, or competitors.
- not sending or receiving data using unsecured/ free public wi-fi
- allowing devices to update when required
- keeping a clear workstation
- using the 'Secure Print' facility on photocopier/ printers when printing confidential or sensitive material.
- taking anti-theft precautions to ensure the physical safety of your device.
- laptop/ mobile users – must take their equipment home every evening after work (Bedford
- office) or put it away in a locked cabinet (Geneva office)

NOT storing confidential or sensitive data -

- o on external hard drives, other storage devices or non-SPD issued devices - unless password protected or encrypted by ARDx IT/ P&G IT;
- o an unsecured hardcopy or similar media.

ONLY storing confidential or sensitive data as follows -

- o digital data on a secure company IT network (within protected/ access limited folders or directories) or qualified 3rd party cloud provider's network with appropriate access controls in place.
- o hardcopy data in lockable cabinets with key safe and key access controls in place

Other generic business safeguards in place to protect the security of our network and business information include:

- assignment of IT equipment and creation/deletion of user accounts in collaboration with the SPD
- HR - New Starter and Leaver processes.
- network access restriction through user ID and strong passwords, with limits set on consecutive
- unsuccessful login attempts.
- controlled physical access to external Data Centres and Disaster Recovery Centres
- remote server data backup and restore processes with data encryption '
- application of security patches and operating system software updates.
- centralised management and whole disc encryption of PCs/ laptops.

Phishing Awareness

Phishing is a technique used by hackers to induce individuals to reveal personal and/or business information, such as passwords and credit card numbers. There are many types of phishing, as listed below:

- Email Phishing (An email sent to multiple people)
- Spear Phishing (An email that targets a particular person or department)
- Smishing (An SMS message sent to people)
- Vishing (A phone call)
- Angler Phishing (Fake Social Media Posts and Pages)
- Whaling (A targeted attack to the people at the top of an organisation)

Phishing attempts can be identified by looking out for:

- The context of the request or message
- Impersonal contacts eg. “Dear User….
- Poor spelling and grammar
- Unexpected, good news (lottery win)
- Subject lines in CAPITAL LETTERS
- Time or hierarchy pressure
- Absence of HTTPS in website links (implies they are not secure)
- Inappropriate email address or phone number of the sender
- Suspicious attachments or weblinks (do not click on these)

If you receive a phishing email, you should report (and forward) it to **phishing@abbott.com** (ARDx IT users) or reportphish.im@pg.com (P&G IT users).

Video Conferencing

SPD have approved the use of MS Teams and WebEx provided by ARDx and P&G for business meetings. Any other applications are not permitted for business use.

To ensure good meeting security you must:

- verify the identity of all participants on calls and allow access only to legitimate external participants being held in the lobby (meeting organisers should remove any participants that have not been successfully dentified).
- ensure any data being shared during screen sharing sessions is appropriate for all the participants on the call.
- check that webcams are deactivated or blocked (e.g., with a sliding shutter) when not required or not in use.
- use the microphone mute function when not actively speaking during a call.
- use the background blur function for personal privacy.
- if meetings are being recorded, all participants must be made aware.

For more information please refer to the Information Technology Usage and Information Security Policy (POLICY-0067).

1.5

Use of Social Media

Social media can bring many benefits in the areas of problem solving, marketing, brand awareness, consumer support etc. However with these benefits there are also significant risks, including inadvertent data and confidential information leakage, copyright breaches and hackers stealing passwords to gain access to company information. Particular care must be exercised when using social media as information and views can spread very quickly and be subject to distortion and misrepresentation, with potentially damaging effects on a company or individual’s reputation.

If you are going to be using any type of social media (e.g. Facebook, Linked-In, Twitter) as part of your job role, there are a number of basic principles that you must follow:

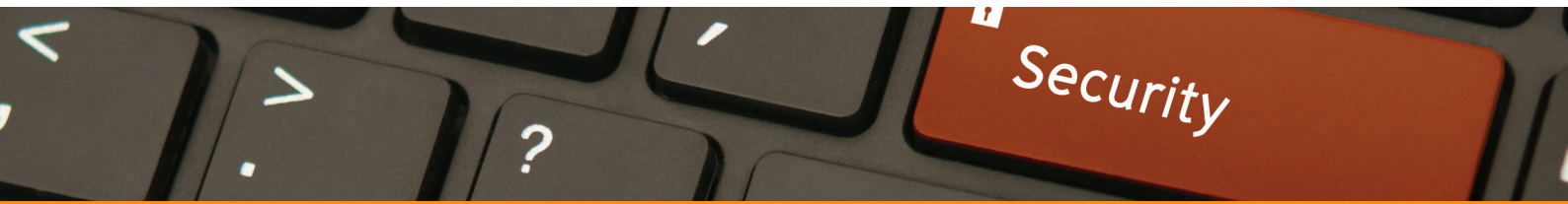
- Get authorisation from the experts: Any new type of internal social media presence and/ or any new external SPD-Sponsored site must first be reviewed by SPD Legal, Regulatory, Customer support and External Affairs
- Protect individual privacy: all activity must comply with relevant Data Protection Laws.
- Be accurate and truthful: never be deceptive or misleading
- Disclose your affiliation with the Company: many laws dictate that persons speaking on behalf of a Company clearly and conspicuously disclose their affiliation
- Only comment on your area of expertise: seek advice from those with appropriate knowledge before commenting in an area that is not your expertise
- **Do not** reveal any of the Company's competitive, confidential, or non-public information: all materials must be approved for external use in the Controlled Document Management System (CDMS)
- Give credit where credit is due and do not violate others' rights: do not claim authorship for something that is not yours and make sure you have the right and permission to use third party materials. If in doubt consult SPD Legal
- Get media trained: if you are engaging in social media activities on behalf of SPD
- Be mindful that you are representing the Company: be professional and respectful of all individuals, ethnicities, cultures and religions
- **Do not** use SPD/P&G passwords as your social media passwords
- **Do not** engage with competitors

Also, when using social media privately please make sure that you:

- **Do not** make postings about our business: only those authorised by SPD should talk about or post material related to SPD or any of our brands
- **Do not** submit consumer reviews for Company products or competitive products: these could be subject to accusations of bias and deceptive business practice by regulators
- Use your personal email address: unless you are interacting on a site used for professional development and association (e.g. Linked-In)
- Know SPD policy if you participate on professional development and association sites: avoid providing opinions on past or current SPD colleagues and/ or their work on professional Social Media business sites
- Protect SPD confidential and proprietary information: do not talk about your job, responsibilities and/or work projects on social media. Use the test "If this were a news headline, would it harm the Company?"
- Use good judgment: your online activities may impact your personal reputation, image and ability to effectively interact with colleagues and business partners
- Respect colleagues, clients, partners and suppliers: do not post anything that they would find offensive, including discriminatory comments, insults or obscenity

Finally, if you are concerned that material posted or proposed to be posted on social media sites may be inconsistent with this policy and/or contain confidential information, contact External Affairs, SPD Legal, or your line manager.

For more information please refer to the Social Media Policy (POLICY-0070).



2

Expectations of SPD in the Workplace

2.1

Health and Safety and the Environment

SPD is committed to ensuring the safety and wellbeing of all its employees, contractors, workplace visitors and immediate neighbours. This is promoted and achieved through collective responsibility by:

- Implementing and maintaining effective controls to minimise and prevent accidents or incidents of work related ill health
- Educating and training employees, contractors and visitors in the competencies required to carry out their work and business safely at SPD sites
- Providing well maintained facilities, resources and equipment to promote a safe and healthy work environment
- Communicating and consulting on day-to-day health and safety issues to raise awareness and proactively reduce risks
- Continually improving the ways we promote health and safety through regular audits/ inspections and acting on our findings
- Having well defined and controlled procedures for the appropriate classification, safe storage, handling and legally compliant disposal of general and hazardous waste generated from our operations

We all have a responsibility both to ourselves and our co-workers to make sure that we understand and follow the SPD Health and Safety policy, its associated systems and controls.

For more information please refer to the Geneva Site Health and Safety Policy (POLICY-0062) and the Health and Safety Handbook (UK) (HSDOC-0015)

2.2

Fairness and Dignity at Work

SPD is committed to providing equal opportunities on all aspects of employment, including:

- Recruitment
- Promotion
- Training
- Pay and benefits
- Disciplinary and grievance
- Selection for redundancy
- Statutory requests for contract variations

As such, SPD does not unlawfully discriminate (either directly or indirectly) on the basis of:

- Age
- Disability
- Sex
- Gender reassignment
- Pregnancy
- Maternity
- Race
- Sexual orientation
- Religion/ belief
- Marital or civil partnership status

SPD is similarly committed to creating a work environment free of harassment and bullying, where everyone is treated with dignity and respect.

Therefore SPD will not tolerate bullying and harassment of any kind, nor will we tolerate victimisation of a person for making allegations of bullying or harassment in good faith.

Allegations of bullying, harassment or victimisation will be investigated and, if appropriate, disciplinary action taken.

For more information please refer to the Employee Handbook

2.3

Ethical Procurement and Social Responsibility in our Supply Chain

SPD is similarly committed to ensuring fair, ethical and safe working practices within its supply chain and requires that its principal suppliers:

- **Do not** engage in or support the use of child labour.
- **Do not** engage in slavery or support the use of forced or compulsory labour, or human trafficking.
- Support the concept of freedom of association and the right to collective bargaining in accordance with local law.
- **Do not** engage in or support discrimination in any form.
- **Do not** engage in or support disciplinary practices that are harsh or inhumane.
- Comply with locally applicable laws on working hours, public holidays and leave.
- Respect the right to a living wage that meets the legal minimum (where established).
- Provide a safe and healthy workplace environment and take effective steps to prevent potential accidents.
- Have procedures and standards for waste management, handling and disposal of chemicals and other dangerous materials, emissions and effluent that meet or exceed minimum legal requirements.

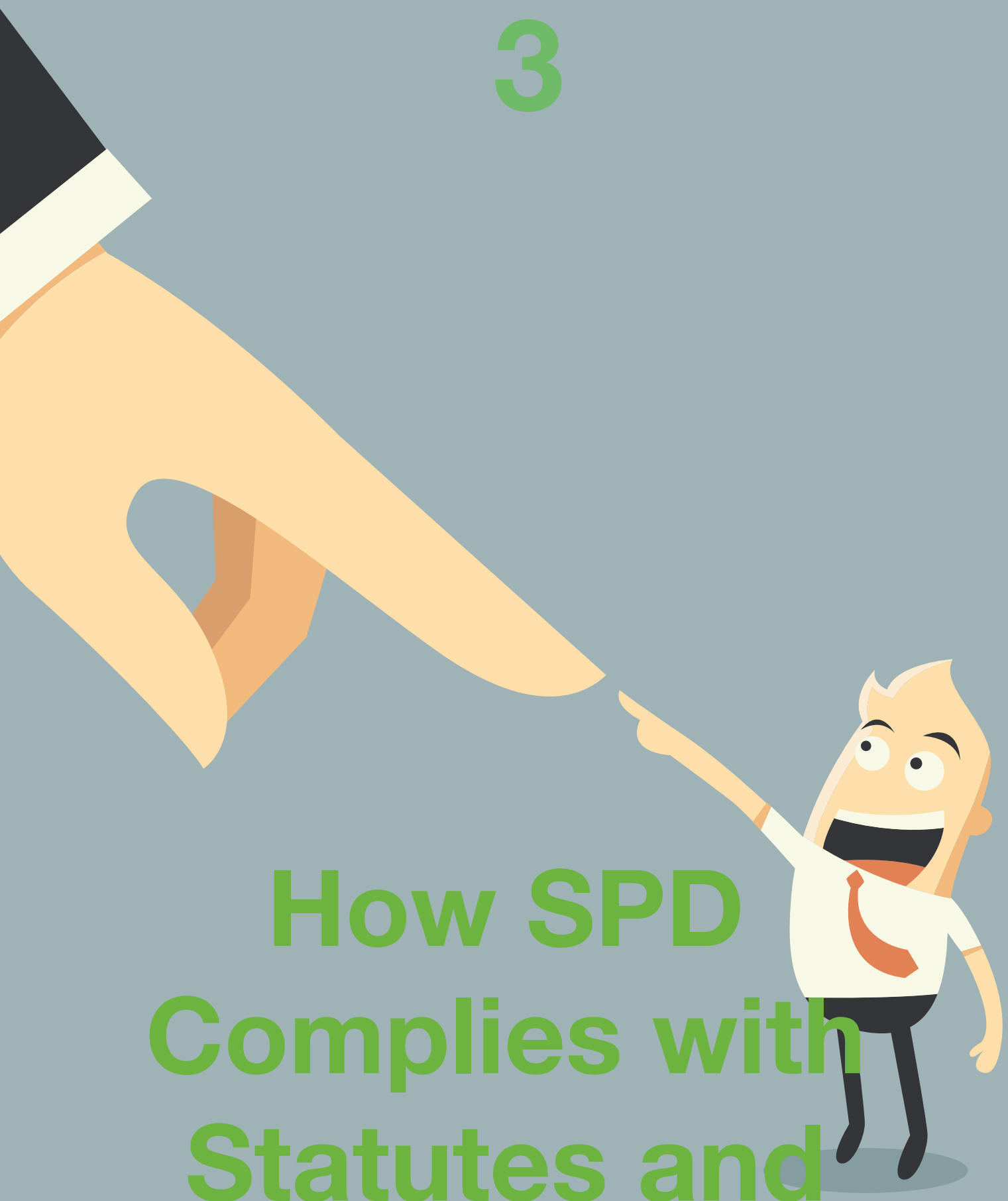
SPD assesses and monitors the compliance of its key suppliers against these requirements by a combination of supplier qualification, self certification, second party audit information, third party audit visits and risk assessment.

Where local legislation and cultural practice are at odds with SPD's policy, SPD will work with suppliers to find sustainable solutions that meet the overall goal of ethical and socially responsible trading.

However, if this is not possible and there is sustained and unacceptable non-compliance with fair employment practices, SPD may terminate the supply.

For more information please refer to the Ethical Procurement/Social Responsibility Policy (POLICY-0063)

3



How SPD Complies with Statutes and Regulations

3.1

Preventing Bribery and Corruption

Compliance with international Anti-Corruption Laws including the UK Bribery Act (2010), the OECD Convention on combating bribery of foreign public officials in international business transactions ("OECD Convention") and the U.S. Foreign Corrupt Practices Act (1977) is an essential component of ethical business conduct.

Violations can lead not only to loss of reputation, but also to considerable fines and criminal penalties for individual employees and company officers.

On a broader scale, corruption undermines democracy, allows organised crime to prosper, disproportionately affects the poor, threatens sustained economic growth and is anti-competitive.

SPD is dedicated to ensuring full compliance with all anti-bribery and anti-corruption laws and regulations.

SPD policy is that no employee, associate or agent of the company shall pay bribes or offer improper inducements to anyone for any purpose, nor do we or will we, accept bribes or improper inducements

It is therefore unacceptable to:

- Give, promise to give, or offer a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given.
- Give, promise to give, or offer a payment, gift or hospitality to a government official, commercial partner, agent or representative to "facilitate" or expedite a routine procedure (aka 'facilitation' or 'grease' payments).
- Accept payment from a third party that you know or suspect is offered with the expectation that it will obtain a business advantage for them.
- Accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided by SPD in return.
- Retaliate against or threaten a person who has refused to commit a bribery offence or who has raised concerns under SPD's Anti Bribery Policy.

Payments made 'under duress' to assure your immediate personal safety are permitted, but should be immediately reported to SPD Legal.

SPD enforces and monitors compliance with its Anti Bribery Policy through a combination of:

- Staff communication and training
- Targeted due diligence during supplier selection and qualification and notification of 'red flags' to SPD Legal
- Contract clauses and warranties within supply agreements requiring commitment from suppliers to comply with anti-corruption laws and actively prevent bribery
- Robust and effective financial controls and maintenance of detailed and accurate financial records
- Adoption of a zero tolerance approach towards any breach of our Anti Bribery Policy and provision of a clear Whistleblowing Policy to enable staff to raise concerns

For more information please refer to the Anti Bribery Policy (POLICY-0071) or contact SPD Legal.

3.2

Money Laundering

SPD is committed to preventing the use of company resources for the purposes of "money laundering," which is an attempt by individuals or organizations to hide the proceeds of their crimes by making those proceeds look legitimate.

This means we must only make payments for goods and services via approved and documented payment processes.

We must be vigilant and exercise good judgment when dealing with unusual supplier or customer transactions, including requests to make payment to a third party or to receive payment from a third party.

Only conduct business with customers and suppliers that are willing to provide you with proper information so that SPD can determine whether the payments are appropriate.

Without appropriate permission from SPD Legal and Finance, you should never:

- Make a payment to an entity that is not a party to the transaction (e.g. third party) or that isn't legally entitled to receive payment.
- Accept a payment from an entity that is not a party to the transaction (e.g. third party) or that isn't legally entitled to make payment.
- Accept payments in cash, unless no secure banking system exists.
- Ship customer orders in a manner inconsistent with standard procedures.
- Conduct foreign exchange operations with unauthorized institutions.
- Make payments without appropriate supporting documentation (e.g. an invoice or similarly documented notice to pay from the entity that is party to the transaction).
- Make payments in the name of another person.

3.3

Fair Dealing and Fair Competition

SPD competes vigorously and effectively based on the superior quality of its products and services.

We never compete unlawfully. For this reason, we must always be truthful in all of our sales and marketing material and we must make only truthful statements about SPD, its products and services.

All marketing claims and other external materials must therefore undergo rigorous internal review by SPD Legal, Regulatory, External Affairs, Marketing and R&D to ensure that they are substantiated by robust evidence and live up to their promises.

We must also abide by competition laws (also referred to as “antitrust” laws). These laws can vary from market to market, but their common goal is to preserve free and open competition and to promote a competitive marketplace. When markets operate freely, consumers benefit through high-quality goods and services at fair prices. Failure to comply with these laws can have serious and far-reaching consequences for SPD and any individuals involved.

As a guide, when interacting with competitors, we must exercise caution and avoid cooperating, or even appearing to cooperate, with them.

We may never discuss any of the following topics with competitors without prior discussion and consent from SPD Legal:-

- Pricing or pricing policy, costs, marketing or strategic plans.
- Proprietary or confidential information.
- Technological improvements.
- Promotions we will conduct with customers.
- Division of customers, markets, territories or countries.
- Boycotts of certain customers, suppliers or competitors.
- Joint behaviour toward customers.

As a guide, when interacting with customers (including both retailers and distributors), we may never:

- Pressure or agree with a customer about resale prices of SPD products (pricing is always at the customer’s sole discretion).
- Terminate a relationship with a retail customer based on threats from or agreements with another retail customer.
- Restrict how, to whom or where customers sell SPD products without the advance approval of SPD Legal.
- Enter into agreements that prohibit a customer from purchasing products from our competitors without the advance approval of SPD Legal.
- Condition the sale of less desirable products with more desirable products (“tying” or “bundling”) without advance approval of SPD Legal.
- Strategize with a customer about specific pricing or promotion of private label products that compete with SPD products.
- Share confidential information of one customer with other customers or help customers coordinate in any way their behaviour on the market.

A firewall is maintained between SPD’s Clearblue Sales and Marketing teams and SPD’s Private Label Sales and Marketing teams to ensure that confidential information (in particular non-public pricing, promotion and other commercially sensitive information) of private label products and customers, and of SPD Clearblue products and customers, which compete with each other, is not shared between these teams and is only used for the purpose for which this information was provided.

This firewall is applied across all SPD to the greatest extent practicable considering that in certain instances support functions may have access to confidential information relating to both Clearblue and Private Label business (e.g. Finance, Legal, Regulatory). Where such access exists, this confidential information shall never be used or shared by such support functions in a way that breaches applicable legislation or any contractual obligation of SPD towards its customers

For more information please contact SPD Legal.

3.4

Quality of Products and Services

SPD's products are regulated in Europe by authorities acting under the European in-vitro Medical Devices Regulations (2017/746) and the European in-vitro Diagnostic Medical Devices Directive (98/79/EC), US FDA under the Code of Federal Regulations (CFR), and globally by country specific regulatory authorities including Health Canada, Australian Therapeutic Goods Administration, Japan's Pharmaceuticals & Medical Devices Agency and ANVISA in Brazil. The laws and regulations enforced by these national regulatory bodies are intended to ensure that medical devices are safe and effective and that these products are honestly, accurately and informatively represented to the public. SPD adheres to these practices through implementation of the Medical Device Single Audit Program (MDSAP) which entails a single regulatory audit to satisfy the relevant requirements of the regulatory authorities participating in the program.

SPD is committed to providing safe, effective healthcare products that meet consumer needs whilst striving to deliver a superior consumer experience and unsurpassed levels of quality, performance and design. Through a culture of personal accountability this commitment is achieved by:

- Setting Quality Objectives and cascading them throughout the organisation
- Continually improving our Quality System and measuring our effectiveness
- Following approved business processes
- Meeting or exceeding international regulatory requirements
- Advancing both technical delivery capabilities and scientific understanding of medical conditions of interest
- Continually building on our in-depth understanding of our consumers needs
- Periodically reviewing how we perform against these commitments

3.5

Protection of Personally Identifiable Information (PII)

SPD is committed to protecting the privacy of its employees and consumers and protecting any Personally Identifiable Information (PII) that it holds in compliance with international Data Protection laws.

PII is defined as any information that identifies an individual – such as name, physical address, email address, employee ID, government ID, photograph, IP address or any combination of this or other information that might identify an individual.

You must not collect, access, use, retain, or disclose PII of SPD employees, consumers, customers, vendors, and/or other stakeholders except when pursuant to relevant and appropriate business purposes e.g. recruitment of volunteers for clinical studies, processing of consumer refunds via Careline, management and maintenance of SPD employee database by HR.

You must store PII on a secure company network. Access should be protected so that only authorized individuals can view and use the information.

Many of the same controls and safeguards previously described for protecting SPD's commercially confidential information should also be applied to the protection of PII (see 1.4 Information Security above).

In addition, PII must **NOT** be stored on any of the following:

- External hard drive or other storage device- unless password protected or encrypted
- Non-SPD issued device - unless password protected or encrypted (consult with your local IT Helpdesk for password protection/ encryption of personal devices)
- Unsecured hardcopy or similar media

When not in use, hardcopy media must be stored on SPD premises in a lockable cabinet, desk, safe or similar furniture

PII must not be shared with anyone, either inside or outside SPD, who does not have a legitimate business need to know or process this data. Furthermore, you should take steps to properly secure such data at all times from unauthorized access by third parties.

Finally, all individual SPD departments that deal routinely with PII must have appropriately documented internal procedures and controls to manage the storage and distribution of this information in accordance with SPD policy.

Anyone who believes that employee, consumer, customer, vendor and/or other stakeholder PII has been disclosed or used inappropriately should contact SPD Legal.

For more information please refer to the Information Technology Usage, Information Security Policy (POLICY-0067) and the Data Privacy Principles (POLICY-0087) or contact SPD Legal.

3.6

Financial Accounts and Records

SPD's parent companies Abbott and P&G rely on us to maintain accurate and detailed financial accounts and records and to ensure that these fairly and completely reflect our operations and financial condition. Reporting accurate, complete and understandable information about SPD's business, earnings and financial condition is one of our most important duties.

We must ensure that our financial statements, regulatory reports and publicly-filed documents comply with all applicable and accepted accounting standards as set out and published by the Financial Reporting Council (UK GAAP), Financial Accounting Standards Board (US GAAP), Swiss Foundation for Accounting and Reporting Principles (Swiss GAAP), statutory requirements and our own internal control procedures.

We regularly review our compliance with these requirements through internal audit/ control self assessment (CSA) and through external audit.

3.7

International Trade Controls - Imports, Exports and Sanctions

SPD works closely with its trading partners to ensure that it complies with all applicable laws and regulations associated with its international trading operations. This includes making sure that all required export licenses and permits are obtained, proper import duties and taxes paid and appropriate customs documentation filed.

From time to time, national governments use economic sanctions and trade embargoes to further various foreign policy and national security objectives. We must be mindful of any sanctions that are in force and ensure that SPD does not breach the terms of any current trade restrictions or embargoes.

If you are unsure whether a transaction complies with all applicable sanction and trade embargo programs, you should contact SPD Legal.

3.8

Third Party Intellectual Property, Copyright and Software Licences

Intellectual Property (IP) refers to creations of the human mind that are protected by law, such as inventions, designs, distinctive brand names, creative works (e.g. music, books, videos) and software.

Collectively, these include copyrights, patents, trademarks, trade secrets, design rights, trade dress, logos, know-how, right of publicity, moral rights, and other intangible property.

SPD respects the intellectual property (IP) rights and other intangible commercial rights belonging to others and we do not knowingly infringe upon those rights in our own technology development, creation of marketing materials or external communications.

Therefore you must always check with SPD Legal before duplicating or using any third party IP.

Furthermore, use of any licenced third-party assets, such as software, music, videos and text-based content, must be in accordance with the specific terms of those licenses and any noted license restrictions.

Company Contact Details

Whistleblowing Hotline

0800 047 4037 (from the UK)

+44 0161 836 9499 (from outside the UK)

Steven Hart

Managing Director
SPD Development Company Ltd
Clearblue Innovation Centre
Priory Business Park,
Stannard Way,
Bedford, MK44 3UP
United Kingdom
Tel: +44 (0)1234 835000
Email: steven.hart@spdspark.com

Veronique Huysmans

General Counsel and Chief Compliance Officer
SPD Swiss Precision Diagnostics GmbH
47 Route de St. Georges
1213 Petit Lancy
Geneva
Switzerland
Tel: +41 58 004 5065
Email: huysmans.v@pg.com