March 2020 Edition

This Policy has the following sections:

## A. INTRODUCTION

1.1 In the course of its business Sangwin Group collects, stores and processes Personal Data about:

1.1.1 its employees (which for the purposes of this Policy includes all agency staff and temporary workers); and

1.1.2 third parties such as suppliers and customers.

Data Protection Legislation ("DP Legislation") imposes certain obligations on us as your employer and on you as our employee relating to how we and you must handle Personal Data irrespective of whether such Personal Data is held on paper, on a computer or on other media.

1.2 In this Policy, Personal Data includes Personal Data which relates to any current, past or prospective employee, supplier or customer or any other person with which Sangwin Group or you have dealings.

1.3 We have prepared this Policy in order to inform you of Sangwin Group's obligations under DP Legislation and your obligations as our employee in respect of the obtaining, handling, processing, storage, transportation and destruction of Personal Data. Each of these activities constitutes "processing" of Personal Data under DP Legislation. This Policy explains how we will process your Personal Data as an employee of Sangwin Holdings Limited and informs you of our rules and procedures for processing third party Personal Data (for example, Personal Data of Sangwin Group customers and suppliers), data security, monitoring and communications.

1.4 This Policy applies to everyone employed by Sangwin Group.

1.5 In this Policy:

1.5.1 DP Legislation means the General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018 and all other data protection legislation having effect in the United Kingdom;

1.5.2 Personal Data means any information identifying an individual or information relating to an individual that can be identified (directly or indirectly) from that data alone or in combination with other identifiers in our possession or which we can reasonably access. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that individual's actions or behaviour; and

1.5.3 Sangwin Group means Sangwin Holdings Limited (CRN: 06687485) and all group companies and subsidiaries of Sangwin Holdings Limited. Sangwin Holdings Limited, is the controller in respect of all Sangwin Group's employee Personal Data and reference in this Policy to "we", "us" and "our" is to Sangwin Holdings Limited unless otherwise stated).

## B THE LAW ON PROCESSING OF PERSONAL DATA - THE KEY PROVISIONS

1.1 The main principles of DP Legislation are that Personal Data must be:

- processed fairly and lawfully and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and up-to-date;
- kept only for as long as it is needed for the purpose for which it was collected; and
- processed in a way that ensures appropriate security of the Personal Data.

All Sangwin Group companies are required to demonstrate compliance with the above principles. In addition, Personal Data must be:

- processed in accordance with the rights of the individual to whom the Personal Data relates; and
- not transferred outside the European Economic Area unless adequate safeguards have been put in place to allow its export.

Please see section 2 of this Policy below for further information about some of the above principles.

1.2 All of this means that all Sangwin Group companies and you must take appropriate measures to ensure that Personal Data is kept secure and handled in accordance with the provisions of DP Legislation. You are responsible for ensuring that any Personal Data you provide to any Sangwin Group company is accurate and up-to-date and that you inform us of any changes to the Personal Data you have provided.

1.3 The Data Compliance Officer for Sangwin Group is David Spurgeon, who is responsible for data protection (tel: 01482 329921; email: david.spurgeon@sangwin.co.uk). Where appropriate, you will receive additional training in respect of our Personal Data handling and security procedures. Any queries relating to this Policy or the handling of Personal Data should be referred to your Sangwin Group company's director or manager in the first instance who will refer the matter on to the Data Compliance Officer if required.

1.4 If you consider that this Policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with the Data Compliance Officer.

### Data Protection Principles

### Fair, Lawful and Transparent Processing

2.1 The intention of DP Legislation is not to prevent the processing of Personal Data, but to ensure that it is processed fairly and without adversely affecting the rights of the individual to which the Personal Data relates. The individual must be informed about, among other things, the identity of the

controller (the relevant Sangwin Group company), the purpose for which the Personal Data is to be processed by that Sangwin Group company, and the identities of anyone to whom the Personal Data may be disclosed or transferred. Such information must be provided through an appropriate privacy notice or fair processing notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that the individual can understand it.

2.2 In order for Personal Data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the individual has consented to the processing, or that the processing is necessary to comply with a legal or contractual obligation, or for the legitimate interest of the controller or the party to whom the Personal Data is disclosed. The processing of special categories of Personal Data (which includes Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data and data concerning health or data concerning an individual's sex life or sexual orientation) is prohibited unless certain conditions are met. In most cases the individual's explicit consent to the processing of such Personal Data will be required.

## Processing for Limited Purposes

2.3 Personal Data may only be processed for the specific purposes notified to the individual when the Personal Data was first collected or for any other purposes specifically permitted by DP Legislation. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the Personal Data is processed, the individual must be informed of the new purpose before any processing occurs.

## Adequate, Relevant and Non-Excessive Processing

2.4 Personal Data should only be collected to the extent that it is required for the specific purpose notified to the individual. Any Personal Data which is not necessary for that purpose should not be collected.

## Accurate Data

2.5 Personal Data must be accurate and kept up to date. Personal Data which is incorrect or misleading is not accurate and steps should be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Personal Data should be destroyed.

## Timely Processing

2.6 Personal Data should not be kept longer than is necessary for the purpose it was collected. This means that Personal Data should be destroyed or erased from Sangwin Group's systems when it is no longer required. For guidance on how long certain Personal Data is likely to be kept before being destroyed or reviewed, please see section 11 of this Policy or contact the Data Compliance Officer.

## Data Security

2.7 All Sangwin Group companies must ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss, destruction or damage to, Personal Data.

2.8 DP Legislation requires all Sangwin Group companies to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data may only be transferred to a third-party data processor if the processor agrees to comply with those procedures and policies, or puts in place adequate measures itself.

2.9 Maintaining information security means guaranteeing the confidentiality, integrity and availability of Personal Data, as follows:

2.9.1 "confidentiality" means that only people who are authorised to use the information can access it. **Personal Data is always considered confidential**;

2.9.2 "integrity" means that Personal Data should be accurate and suitable for the purpose for which it is processed; and

2.9.3 "availability" means that authorised users should only be able to access the information if they need it for authorised purposes. Unless otherwise agreed with the Data Compliance Officer, Personal Data should be stored on Sangwin Group's central computer system and not on individual PCs.

2.10 Security procedures include (but are not limited to):

2.10.1 Entry controls - any stranger seen in entry-controlled areas should be reported.

2.10.2 Secure lockable desks and cupboards - desks and cupboards should be kept locked if they hold confidential information of any kind.

2.10.3 Methods of disposal - paper documents containing confidential information should be shredded. Digital storage devices should be physically destroyed when no longer required.

2.10.4 Equipment - staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

2.10.5 Encryption - all Sangwin Group servers and portable devices are encrypted before use to protect confidential information in the event of unauthorised access.

2.10.6 Data minimisation - all Sangwin Group companies periodically review the Personal Data they hold. Any Personal Data which that company no longer needs, or which is held outside the retention periods detailed in this Policy will be disposed of.

2.10.7 Anonymisation / pseudonymisation - where appropriate, Personal Data should be anonymised or pseudonymised.

2.10.8 System checks - Sangwin Group's IT systems are protected by Sophos End Point Anti-Virus software and Sonicwall Network Security and are regularly tested for security threats and viruses and updated as appropriate. Email is protected by Microsoft 365.

2.10.9 Sangwin Group's IT systems are backed up in accordance with the Group Disaster Recovery Policy in order that they can be restored in a timely manner in the event of a physical or technical incident.

### Processing in Line with the Rights of Individuals

2.11 Personal Data must be processed in line with individuals' rights. Individuals must be provided with information regarding the processing of their Personal Data and (subject to limited exemptions) have a right to:

2.11.1 request access to any Personal Data held about them by a controller (including but not limited to Personal Data held within their personnel file); and

2.11.2 rectification of inaccurate Personal Data.

In certain circumstances, individuals may also have the right:

2.11.3 to erasure of Personal Data;

2.11.4 of data portability (i.e. to request the transfer of Personal Data to another party);

2.11.5 to object to the processing of Personal Data concerning him or her (including to prevent the processing of their Personal Data for direct marketing purposes);

2.11.6 not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her;

2.11.7 to restrict the processing of Personal Data (for example to ask to suspend the processing of Personal Data to establish its accuracy or the reasons for processing it).

## C. HOW SANGWIN HOLDINGS LIMITED PROCESSES PERSONAL DATA OF ITS EMPLOYEES

### Your Personal Data

3.1 As your employer we hold Personal Data about you which we have received either from you (for example, through the application and recruitment process) or from a third party such as your previous employer. The Personal Data we may collect, store and use about you includes: personal details such as name, title, addresses, telephone numbers and personal email addresses; date of birth; gender; marital status and dependants; next of kin and emergency contact information; National Insurance number; bank account details; payroll records and tax status information; salary, annual leave, pension and benefits information; start date; location of workplace; copy of driving licence; recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process); employment records (including job titles, work history, working hours, training records and professional membership); compensation history; performance information; disciplinary and grievance information; CCTV footage; information about your use of our information and communications systems; and photographs.

We may also collect, store and use the following special categories of more sensitive Personal Data: information about your race or ethnicity; religious beliefs; sexual orientation and political opinions; trade union membership; information about your health including any medical condition; health and sickness records; information about criminal convictions and offences. We need the Personal Data listed above for a number of reasons, including (but not limited to):

3.1.1 to perform our obligations under your employment contract (for example, to arrange payment of your wages and to provide you with any benefits detailed in your employment contract);

3.1.2 to comply with a legal obligation to which we are subject (for example, to check you are legally entitled to work in the UK and to comply with health and safety requirements);

3.1.3 where it is necessary for the purposes of our legitimate interests and your interests and fundamental rights do not override those interests (for example, to conduct performance reviews, make decisions about salary reviews and compensation, to gather evidence for possible grievance or disciplinary hearings, to assess education, training and development requirements, to monitor your use of our information and communication systems to ensure compliance with our policies and procedures and to prevent fraud);

3.1.4 where it is necessary for the purposes of us carrying out our obligations and exercising our or your rights under employment law or for the assessment of your working capacity (for example, data concerning health in order to monitor and manage sickness absence and ascertain your fitness for work, and information about your racial and ethnic origin and religious or similar in order to monitor our compliance with equal opportunities legislation);

3.1.5 where it is necessary for the establishment, exercise or defence of legal claims by us; or

3.1.6 where it is necessary to protect the vital interests of you or another person where you are physically or legally incapable of giving us consent.

The majority of the Personal Data we hold about you is contained in either your employment records or in your personnel file, hard copies of which are held by the wages clerk, for weekly paid employees and by the finance director for all other employees. Only authorised personnel have access to your personnel file Personal Data relating to salary, bonuses, benefits, pensions, tax codes and other Personal Data necessary for us to calculate your monthly salary is also stored electronically and can only be accessed by authorised personnel.

3.2 You will be asked before we disclose your Personal Data to third parties, unless:

3.2.1 the company is part of the Sangwin Group (all of which are located within the EEA);

3.2.2 they are only acting as our processor. The following activities are carried out by third party processors on our behalf: pension administration and IT services;

3.2.3 such disclosure is required by law;

3.2.4 the third party is providing us with professional advice where permitted by law;

3.2.5 the disclosure is in connection with any criminal investigation where permitted by law;

3.2.6 the disclosure is in connection with any legal proceedings or prospective legal proceedings where permitted by law;

3.2.7 the disclosure is in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk) where permitted by law;

3.2.8 the disclosure is necessary to protect the interests of you or another person where you are physically or legally incapable of giving us your consent;

3.2.9 the disclosure is in connection with a proposed sale of any business or assets (in which case we may disclose your Personal Data to the prospective seller or buyer of such business or assets) or the proposed acquisition of substantially all of our assets by a third party.

3.3 If you wish to make a request in relation to your Personal Data pursuant to paragraphs 2.11.1 to 2.11.7 above, such request should be made in writing to the Data Compliance Officer who will respond to your request as soon as possible and, in any event, within one month from the date of receiving the request. You will not have to pay a fee to exercise any of your rights set out in paragraph 2.11. However, we may charge a reasonable fee if your request to access your Personal Data is clearly unfounded or excessive. Alternatively, we may refuse to comply with your request in such circumstances.

## D. HOW EMPLOYEES OF SANGWIN HOLDINGS LIMITED MUST HANDLE PERSONAL DATA OF THIRD PARTIES

### What You Can And Cannot Do With Personal Data Of Others

4.1 All information (including but not limited to Personal Data) relating to Sangwin Group's employees' suppliers, and customers and any other person with whom any Sangwin Group company or you, in your role as our employee, have dealings is confidential information and belongs to the relevant Sangwin Group company.

4.2 You must not access such information unless we have given you permission to do so.

4.3 Information about Sangwin Group's employees, suppliers and customers must not be disclosed to any third party or to the person to whom it relates except in accordance with this Policy and our authorised procedures. For example, you must never assume that it is acceptable for a husband to be given Personal Data about his wife; they may be estranged or simply wish to keep their affairs separate. **In the event that you receive a request from a third party for disclosure of, or to inspect, Personal Data relating to any individual (including but not limited to employees, customers or suppliers) you should refer the request to the Data Compliance Officer immediately**. You should make such a referral in all cases and should not respond to the request regardless of the identity of the requestor (including where the requestor is the police or any other government agency or public authority) as we have a set procedure for responding to such requests that must be followed.

4.4 Subject to paragraph 4.3 above, if you are in any doubt as to the identity of an individual, you must verify his or her identity before disclosing Personal Data to him or her. In any event, you should never give any Personal Data to anybody over the telephone regardless of the identity of the person making the request.

4.5 When making electronic records of Personal Data you must save them in the relevant areas of Sangwin Group's computer network and not locally on the workstation's hard drive. Manual records must be stored in a secure filing system.

4.6 Subject to paragraph 7.9 which concerns contractual negotiations by email, hard copies of information should not be taken from the computer network unless absolutely necessary and where they are taken they must be kept in a secure location.

4.7 You must not leave information relating to Sangwin Group's employees, suppliers or customers in open view where others can see it. For example:

4.7.1 computer terminals at locations where people other than sufficiently authorised employees can see them should not be left unattended. The screen should not be visible to any third party except as required to carry out the transaction in question;

4.7.2 if you take payment and/or financial details from a customer away from our premises you must ensure that the payment and/or other personal details are kept in a secure place away from public view until they can be stored appropriately as soon as possible after you return to our premises.

4.8 Personal Data must not be copied manually or onto an electronic storage device (such as a CD-ROM, DVD-ROM, USB key or MP3 player) except as specifically authorised by the Data Compliance Officer. In the event that any information is copied onto any such device it must be encrypted before being removed from our premises. CD-ROMs and DVD-ROMs should be physically destroyed when they are no longer required.

4.9 If you use a tablet computer or other hand-held device away from our premises you must take appropriate additional precautions to safeguard the security of Personal Data. Such precautions include but are not limited to keeping the device either with you or in a secure location at all times. Documents, tablet computers and other devices containing Personal Data should never be left unattended in vehicles (even when the vehicle is parked at your home). In the event that any such device is lost or stolen, or you believe that it may have been accessed by an unauthorised person or otherwise compromised, you must report it to the Data Compliance Officer immediately.

4.10 In the event that you are provided with a company mobile telephone, laptop, tablet computer or similar electronic device, you shall only use such a device in accordance with our instructions and you shall not use such a device for any unauthorised purpose.

4.11 Care must be taken when synchronising any portable device such as a tablet computer with the relevant parts of our computer network that you only synchronise with those parts of the network which you are authorised to access.

4.12 You must not send or copy any confidential information relating to any Sangwin Group company (including but not limited to Personal Data about our employees) or its customers or suppliers to any third party without specific authorisation from a Director. This includes sending or copying information to any non-Sangwin Group email address and any device or system not owned and operated by a Sangwin Group company.

4.13 Desks and cupboards should be kept locked if they hold confidential information of any kind.

4.14 You must comply with our confidential waste disposal procedures (such as shredding) and ensure that confidential documents, including receipts and invoices, are not simply disposed of with the non-confidential waste.

4.15 Tapes and disks must be cleansed or destroyed by Sangwin Group's IT department after use. Simply deleting information from them does not prevent the information from being recovered at a later date.

4.16 Any formal request from an individual for Personal Data that any Sangwin Group company holds about them, and any other correspondence of the nature referred to in paragraphs 2.11.1 to 2.11.7

above, must be made in writing. Any member of staff who receives a written request should forward it to the Data Compliance Officer immediately and not respond directly to the request.

4.17 We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

## E. USE OF PASSWORDS

### Passwords

5.1 Where we consider it necessary you will be issued with a password so that you can access information (which may include Personal Data) held within restricted parts of our computer network. In any event, you must not disclose your password to anyone else. Passwords are for our benefit and are our proprietary and confidential information.

5.2 If you suspect that any of your passwords may no longer be secure, you must immediately change any such password and notify Sangwin Group's IT department in order that the previous password(s) can be disabled.

5.3 You must log off the network when you leave our premises and initiate a password-protected screensaver when you leave your computer unattended to prevent anyone else accessing the network using your log-in identity. If you do not, you may be deemed to be the person accessing the network unless you can prove otherwise. You must also ensure that your monitor does not show confidential information to passers-by.

5.4 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

## F. USE OF THE INTERNET, EMAIL, TELEPHONE AND POST

### The Internet

6.1 Your use of the Internet (including but not limited to social media postings), whether on our premises or by remote access, may be monitored by us to ensure that our rules are being complied with and for legitimate business purposes. Any personal, non-business activities carried out using Sangwin Group's IT facilities shall be done at your own risk with no expectation of privacy. Do not use Sangwin Group's IT facilities and communications systems for any matter that you wish to be kept private or confidential.

6.2 You can access the Internet for reasonable personal use during recognised break times provided that such use does not interfere with your normal day-to-day duties or the operation of our business.

6.3 You must not access, transmit, save or reproduce illegal, defamatory, offensive, obscene, demeaning, indecent, disruptive, discriminatory or sexually explicit material. If you discover such material, you must inform Sangwin Group's IT department as soon as possible as your computer automatically stores a copy of the material which must be removed.

6.4 Downloading and installing files or software (including but not limited to via the Internet) is permitted only where it is for our business purposes and Sangwin Group's IT department has approved the

download. All files, programs and software downloaded must be checked for computer viruses before being opened.

6.5 Certain material, especially software, text and images downloaded from the Internet, may be protected by copyright. Permission must be obtained from the copyright owner before such material is downloaded. Unlicensed software must not be downloaded.

6.6 You must not establish Internet or other external communications connections that could enable a third party to access our computer systems.

6.7 You must not access external networks or other computers via Sangwin Group's network without prior permission.

6.8 When connecting to the Internet using a portable device such as a "dongle" on a laptop computer it is your responsibility to ensure that you terminate the Internet connection as soon as you have completed the relevant task.

6.9 Any requests for references that you receive must be referred to your relevant manager. In particular, you should never provide references for any other individual on social or professional networking sites, as such references (whether positive or negative) can be attributed to us and create legal liability for both us and you as the author of the reference. References should not be given about an individual to a third party unless that individual has provided consent.

## Email and Other Correspondence

7.1 Sangwin Group's computer network and email system is the property of the relevant Sangwin Group company and all emails sent and received, including by remote access, may be subject to access and monitoring by us at any time at our discretion. We may also delete messages or prevent messages being sent from the email system at our discretion and we may disclose details about your use of email and the Internet as required to comply with the relevant Sangwin Group company's legal and contractual obligations with its communications service providers.

7.2 If you need to access another employee's computer or mailbox, or to allow another employee to access your computer or mailbox, you must first obtain authorisation from Sangwin Group's IT department to do so.

7.3 You must not, and must not attempt to:

7.3.1 create, display, store, copy, send or forward:

(a) illegal, defamatory, obscene, derogatory, demeaning, menacing, threatening, abusive, indecent, disruptive, discriminatory or sexually explicit images, data, text or other material, including but not limited to regarding race, sex, religion, colour, national origin, marital status, age, physical or mental disability, medical condition or sexual orientation;

(b) material which is designed, or which is likely, to cause offence, annoyance, harassment, inconvenience or anxiety;

(c) electronic chain mail;

(d) anonymous mail or mail which is forged to misrepresent the identity of the sender;

(e) material which infringes the intellectual property rights of a third party. If in doubt consult Sangwin Group's IT department before sending such material; or

(f) advertising material (whether solicited or not) unless you have permission from us to do so.

7.3.2 infect Sangwin Group's or third parties' systems with computer viruses;

7.3.3 do anything which hinders the ability of other employees to use Sangwin Group's email system; or

7.3.4 use the email system to solicit others for commercial ventures or for religious, charitable or political causes, or for operating as a personal business, or for any illegal or wrongful purpose.

7.4 If you receive material of the type described in paragraph 7.3.1 you should contact Sangwin Group's IT department as soon as possible as your computer automatically stores a copy of the material which must be removed.

7.5 You may use the email system for reasonable personal use provided that such use does not interfere with your normal day-to-day duties or the operation of our business.

7.6 Outgoing emails bear the name of Sangwin Group or another of our brand names and therefore impact on our image. You should always be professional and courteous when communicating by email and should spell check and proof read emails before sending them.

7.7 Personal comments and opinions in correspondence and other documents should be avoided wherever possible as individuals have the right to request copies of all of the Personal Data that we hold about them, including such written comments and opinions. All email messages may be disclosed in legal proceedings in the same way as paper documents, and should be treated as potentially retrievable even after they have been deleted.

7.8 It is possible for legally binding contracts to be made or varied through email correspondence. If you are involved in any form of contract negotiation you must obtain the permission of a Director before using email to correspond on any contractual terms. Where appropriate, you should expressly state the limitations on the extent to which your messages are sent on our behalf.

7.9 Where you are negotiating contractual terms by email, where appropriate you should print a hard copy of each email. Otherwise emails should not be printed out unless absolutely necessary. Printed emails must always be stored in the relevant secure file.

7.10 Electronic copies of emails should generally only be retained in your inbox or elsewhere on the computer network for as long as they are needed for the purpose for which they were sent or received.

7.11 Only Directors and their designated representatives are permitted to sign documents on Sangwin Group's behalf or otherwise bind any Sangwin Group company to agreements.

7.12 **Incoming emails that contain attachments could contain viruses. Do not open attachments without first checking to ensure that they are virus-free unless you are certain that they originate from a safe source. All incoming e-mails are automatically scanned for viruses by Sangwin Group's IT system and the results of each anti-virus scan can be found at the footer of the relevant e-mail. If no such results**

**can be seen in any e-mail that you receive, please contact Sangwin Group's IT department and do not open any attachments to the e-mail unless Sangwin Group's IT department tells you that it is safe to do so.**

### Telephone Use

8.1 The telecommunications system (including land lines and mobile phones provided by us) is Sangwin Group's property and any calls made to or from it may be subject to monitoring at any time at our discretion.

8.2 The making and receiving of private telephone calls must be kept to a minimum and is only permitted where such calls do not go beyond what we regard as reasonable use and do not interfere with your normal day-to-day duties or the operation of our business.

8.3 In order to monitor the use of Sangwin Group's telecommunications systems and to assist in managing costs and employee time, we ask Sangwin Group's telecommunications providers to itemise all land line and mobile telephone bills on a monthly basis. You may be asked to identify telephone numbers of calls made from telephones owned or leased by us and the nature of such calls.

### Post

9.1 All post received at our premises, whether or not marked strictly private and confidential and/or for the attention of an individual employee, may be opened and inspected prior to distribution. You should be mindful of this if you ask for personal items or correspondence to be delivered to our premises.

## G. SANGWIN GROUP'S USE OF CCTV

### Use of CCTV

10.1 Sangwin Group currently uses CCTV cameras to view and record individuals on and around Sangwin Group's premises. Sangwin Group believes that such use is necessary for legitimate business purposes, including:

10.1.1 to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;

10.1.2 for the personal safety of employees, visitors and other members of the public and to act as a deterrent against crime;

10.1.3 to support law enforcement bodies in the prevention, detection and prosecution of crime;

10.1.4 to assist in day-to-day management, including ensuring the health and safety of employees and others;

10.1.5 to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;

10.1.6 to assist in the defence of any civil litigation, including employment tribunal proceedings; and

10.1.7 for insurance purposes.

This list is not exhaustive and other purposes may be or become relevant.

10.2 Sangwin Group has considered alternatives to using CCTV, such as additional regular inspections of Sangwin Group's premises, but has concluded that such alternatives would be less effective and more costly. In particular, there are situations which will require a rapid response if the risk to employees' security and safety is to be minimised. CCTV is the best way for Sangwin Group to achieve this.

10.3 Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. The CCTV cameras will not be used to record sound.

10.4 Only authorised personnel have routine access to live and recorded images generated by the CCTV cameras. Such authorised personnel will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

10.5 The relevant Sangwin Group company shall display prominent signs at premises where CCTV cameras are present unless in exceptional circumstances it is deemed necessary not to do so. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

10.6 In the event of there being any damage, theft or trespass affecting our developments, recorded images will be provided to law enforcement authorities where appropriate. The relevant Sangwin Group company may use recorded images as evidence in misconduct and performance-related investigations as well as in disciplinary and court proceedings. Images will not be used or released for any commercial or entertainment purpose.

10.7 The CCTV camera's monitoring and control equipment is located securely at The Sangwin Group's Head Office, Dansom Lane South, Hull HU87LN and 56 Dansom Lane South, Hull, HU8 7LA

10.8 Images will not be removed from the CCTV system itself other than in accordance with this CCTV policy. All images recorded using the system will be held for 30 days and then deleted automatically. If any images are provided to law enforcement authorities, this shall be achieved by providing an electronic copy of the recording to the relevant authority.

10.9 All requests for access to images recorded using Sangwin Group's CCTV system should be made in writing in accordance with section 4.16 above. In order for the relevant Sangwin Group company to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

10.10 Sangwin Group will ensure that the ongoing use of existing CCTV cameras as set out above is reviewed periodically to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

10.11 Please contact the Data Compliance Officer if you have any queries about Sangwin Group's use of CCTV.

## H. RETENTION PERIODS IN RESPECT OF PERSONAL DATA

### 11. How long Sangwin Group retains Personal data

Each Sangwin Group company will only retain Personal data for as long as it needs it for the purpose for which is was collected. Whilst taking in to consideration its legal obligations, each Sangwin Group company will on an ongoing basis: review the length of time it retains Personal Data; consider the purpose or purposes for which it holds the Personal Data for in deciding whether (and for how long) to retain it; securely delete Personal Data that is no longer needed for such purpose or purposes; and update, archive or securely delete information if it goes out of date. The following table sets out Sangwin Group's current retention periods:

| Personal Data | Special Categories of Personal Data | Retention Period | Reason |
|---|---|---|---|
| Staff personnel records including training records and disciplinary / grievance hearings | Yes | 6 years from the end of employment (except where a claim relating to the individual has been made or notified in that period, in which case the retention period may be extended as necessary to deal with the claim) | Time limits on litigation (s.5 Limitation Act 1980) |
| Job Application forms and Interview notes | Yes | 6 months from the date that the candidate is notified of whether or not they are successful (except where a claim relating to the individual has been made or notified in that period, in which case the retention period may be extended as necessary to deal with the claim) | Time limits on litigation (s.123 Equality Act 2010) |
| Disclosure and Barring Service (DBS), formerly Criminal Records Bureau (CRB), checks and disclosures of criminal records forms | Yes | Delete following recruitment process unless assessed as relevant to ongoing employment relationship. Once a conviction is spent, should be deleted unless it is an excluded profession | Rehabilitation of Offenders Act 1974 & Information Commissioner's Employment Practices Code |
| Facts relating to redundancies | No | 6 months from the end of employment (except where a claim relating to the individual has been made or notified in that period, in which case the retention period may be extended as necessary to deal with the claim) | Statutory time limit for making a redundancy claim (Employment Rights Act 1996) |
| Income Tax and NI returns; Correspondence with Tax Office | No | 6 years from the financial year-end in which payments were made | Schedule 18 para 21 Finance Act 1998 (as such records may fall within the definition of payroll and wage records) |

| | | | |
|---|---|---|---|
| Statutory Maternity Pay records and calculations | No | 3 years after the end of the tax year in which the maternity pay period ends | Regulation 26 Statutory Maternity Pay (General) Regulations 1986 |
| Statutory Sick Pay records and calculations | Yes | 3 years after the end of the tax year to which the records relate | Regulation 13A Statutory Sick Pay (General) Regulations 1982 |
| Payroll and wages records | No | 6 years from financial year-end in which payments were made | Schedule 18 para 21 Finance Act 1998 Finance Act 1998 |
| Records and reports of accidents / deaths / injuries in connection with work | Yes | 3 years after the date the relevant incident was reported | Regulation 12 Reporting of Injuries, Diseases, and Dangerous Occurrences Regulations 2013 |
| Health Records for any person who was not at any time during their employment placed under health surveillance | Yes | 3 years from the end of employment (except where a claim relating to the individual has been made or notified in that period, in which case the retention period may be extended as necessary to deal with the claim) | Statutory limitation period for personal injury claims (s.11 Limitation Act 1980) |
| Health records for any person who was placed under health surveillance at any time during their employment | Yes | 40 years from the date of the last entry (except where a claim relating to the individual has been made or notified in that period, in which case the retention period may be extended as necessary to deal with the claim) | The Control of Substances Hazardous to Health Regulations 2002 |

## I REPORTING BREACHES OF DATA PROTECTION LEGISLATION

### What you should do if you discover a data protection breach

If you become aware that:

11.1 a device has been lost or stolen, or if you believe that a device may have been accessed by an unauthorised person or otherwise compromised;

11.2 there has been unauthorised access to any element of Sangwin Group's IT system, premises or any other location where Personal Data is stored;

11.3 any Personal Data has been disclosed or accessed in error;

11.4 there is an IT threat (for example, if you have received a phishing email);

11.5 Personal Data has been compromised in any other way,

you must report the incident to the Data Compliance Officer immediately. In some circumstances we may be required to report the breach to the Information Commissioner's Office and the individual(s) concerned.

## J. ADDITIONAL INFORMATION

### General

12.1 This Policy does not form part of any employee's contract of employment and it may be amended by us at any time. Any changes will be notified to you in writing.

12.2 If you are found to be in breach of the terms of this Policy you may be subject to disciplinary proceedings which in serious cases, or in cases of repeated breach, may result in dismissal. If you are in any doubt about the terms of this Policy or have any questions about data handling, data security, monitoring or communications, please ask the Data Compliance Officer for further guidance.

12.3 Sangwin Group's IT department can be contacted by calling 01482 329921, emailing rob.tolson@sangwin.co.uk or help@theonepoint.co.uk or writing to Rob Tolson, Sangwin Group, Dansom Lane South, Hull HU8 7LN.

12.4 We will continue to review the effectiveness of this Policy to ensure it is achieving its stated objectives.