Welcome to the Davidson Richards Limited's privacy notice.

Davidson Richards Limited respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data and tell you about your privacy rights and how the law protects you.

Please use the Glossary at the end of this privacy notice to understand the meaning of some of the terms used in this privacy notice.

1 Who we are

Controller

Davidson Richards Limited is the controller and responsible for your personal data (referred to as ”DRL” "we", "us" or "our" in this privacy notice).

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the privacy manager using the details set out below.

Contact details

Our full details are:

Full name of legal entity: Davidson Richards Limited

Name or title of data privacy manager: Chris Worthington

Email address: data@davrich.co.uk

Postal address: Systems House, The Parker Centre, Mansfield Road, Derby, DE21 4SZ

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

2 The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

(a) Identity Data includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.

(b) Contact Data includes billing address, delivery address, email address and telephone numbers.

(c) Financial Data includes bank account details.

(d) Transaction Data includes details about payments to and from you and other details of products and services you have purchased from us.

(e) Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.

(f) Profile Data includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.

(g) Usage Data includes information about how you use our website, products and services.

(h) Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

This website is not intended for children and we do not knowingly collect data relating to children.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

3 How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions.** You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- apply for our products or services;
- create an account on our website;
- subscribe to our service or publications;
- request marketing to be sent to you;
- enter a competition, promotion or survey; or
- give us some feedback.
- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies.
- **Third parties or publicly available sources**. We may receive personal data about you from various third parties and public sources as set out below:
- Technical Data from the following parties:

(a) analytics providers such as Google based outside the EU;

(b) search information providers such as Google based outside the EU].

- Identity and Contact Data from publicly availably sources such as Companies House and the Electoral Register based inside the EU.

4 How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

Generally we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include: (a) To supply services to you (in relation which see below for more information) (b) Notifying you about changes to our terms or privacy policy (c) Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To enable you to partake in a prize draw, competition or complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)

	(e) Marketing and Communications (f) Technical	
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)

Marketing

Prospective lists of businesses (not individual consumers) are purchased from reputable sources which have been screened for CTPS membership (Corporate Telephone Preference Service) or from Trade Associations that we are members of.

We also subscribe to a TPS telephone number checking service.

This is controlled by our Marketing Manager.

Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased goods or services from us or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

Such personal data may include, but is not limited to, the following categories:

- First and last name
- Job title and position
- Contact information (company name, email, telephone, physical business address, fax number)
- Professional data
- Membership of trade associations
- Notes from telephone calls & other activities

This information is retained without limit whilst a legitimate business need may exist for our products and services given that the typical timescale for review of our solutions or services may take several years.

We use Microsoft CRM 365 for our customer relationship management software. Access to this web-based solution is via a unique login password for each member of staff.

This is controlled by our Marketing Manager.

Enewsletters

Our enewsletter system is provided by BinaryFold4 Ltd. This is used to communicate with existing customers, our software partners and prospective business customers.

Such personal data may include, but is not limited to, the following categories:

- First and last name
- Email address
- Company name
- Business application used (for customers or prospective customers)
- Membership of trade associations

Our enewsletter and other marketing communications' footers provides an unsubscribe button which (if used by the recipient) will automatically unsubscribe the recipient from that list and prevent future communications.

Details can also be deleted manually upon request.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product/service purchase or experience or, other transactions.

This information is retained by us until an existing customer leaves us or choses to unsubscribe or a prospective customer chooses to unsubscribe, or we delete the customer records (if their business has been acquired for example whereby there is no longer a legitimate need for our service).

Access to the web-based application is via a unique login password for each member of staff.

This is controlled by our Marketing Manager.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5 Disclosures of your personal data

We may have to share your personal data with the parties set out below for the purposes set out in the table in paragraph 4 above.

- External Third Parties as set out in the Glossary.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

Customer Information Shared with Third Parties

While working for our customers, we may need to share information with trusted third parties. For example, for our retail customers, we may need to share information with the customer's Electronic Funds Transfer (EFT) provider.

HTA

For our customers from the garden centre sector, we can provide our retail solutions integration software which allows our customers to sell the Horticultural Trade Association (HTA) gift cards and gift check card balances.

This is at the customer's request and is initiated either by the customer themselves to us or via the HTA who then contact us so that we can arrange the integration.

To activate this software within our solution, with the customer's permission, we act as the liaison point between the customer, the HTA and EML who authorise the gift cards on behalf of the HTA. Information shared between the parties is:

- name
- address
- contact name
- telephone number(s)
- email

The HTA provide us with the customer's HTA reference which we need for our software integration configuration.

EML provide us with the Store ID for that customer and grant permission so that our OpServices software integration can communicate when checking gift card balances and for EML to authorise the card once a value has been purchased to load onto it. No personal details are transmitted or stored as part of our integration.

When redeemed in-store, the HTA gift card payments are authorised by the EFT Chip and Pin acquirer our customer's use as they are MasterCards.

The data is accessed via a unique login password and is transmitted via a secure network (https).

The customer (retailer), HTA and EML adhere to anti-money laundering regulations. This is controlled by our Operations Director.

Hosting

Our OpSuite retail management and EPoS solution operates in the environment provided by our hosting partner, UK Fast. The data held in OpSuite is customer-defined.

For our customers using our OpSuite retail management and EPoS solution, all our customers' data is securely controlled and held on cloud-based servers at UK Fast Ltd which process the data within the EEA.

The OpSuite data, which includes an enterprise's customer details and transactions, is held in Microsoft SQL Server databases hosted on servers in the secure location at UKFast's data centres in Manchester.

The data centre implements various industry standard levels of physical and virtual security as detailed here https://www.ukfast.co.uk/our-datacentres.html.

The database server is on a private network that is not available to the outside world. The data is also backed up within the UKFast centre.

Access to the data over the internet is made available via web sites and web services that are also hosted on servers at UKFast. Requests to these sites and services are over HTTPS (hypertext transfer protocol secure communication) and require that the request contains credentials that first need to be authenticated before the request is accepted.

The DRL staff can also access the data through direct secure connection to the SQL databases.

UKFast also hold ISO 27018 certification which compliments much of the data processing responsibilities set out by the GDPR. It aims to protect personal data in additions to EU requirements and it applies to cloud service providers.

When an OpSuite customer leaves us, we can upon request export their data and transfer the files by way of the secure method outlined in this document. Once the monthly subscriptions have ended or as agreed, access to the cloud-based customer database will be disconnected. Given the time to be removed from back-ups etc. the customer information will be deleted from our system within 3 months.

This is controlled by our Operations Director.

6 International transfers

We do not transfer your personal data outside the European Economic Area (EEA).

7 Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We ensure an adequate level of security by considering industry standard and practices, the nature, scope, context and purposes of processing activities and the risks to individual privacy. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Our technical and organisational measures include: secure user authentication protocols, user access control measures; secure data file transfer protocols, secure storage of data; and education and awareness training of employees on the proper use of computer security systems and the importance of personal data protection.

Partners

Davidson Richards has a partner channel for its software solutions.

A partner may send personal data to Davidson Richards to make purchases, receive services or support and manage the business relationship. For example, for administration, billing & payment, credit control, support, marketing, account management purposes or the contract in place.

Such personal data may include, but is not limited to, the following categories for themselves and their customers using our software or solutions:

- Partner Company Name
- Address(es)
- Fax No
- Telephone number(s)
- Email address
- Contact information (first and last name(s), job title(s), email(s), telephone number(s),
- BACS/bank account name, sort code & account number
- Passwords for use in providing our support or other services

The above information will be retained where there is a legitimate business or a legal need to do so. This includes compliance with our legal requirements, dispute resolution, enforcement of agreements, for other lawful business purpose or in line with statutory requirements.

We use Pegasus Opera 3 / Historical Pegasus Opera System for contract management.

The information is located on a secure domain authenticated network accessed by a unique login password for each member of staff.

This is controlled by our Department Managers, Operations Director & Company Secretary.

Suppliers

A supplier may send personal data to Davidson Richards for us to make purchases, receive services or support and manage the business relationship. For example, administration, supply of goods or services, billing & payment or relating to the contracts in place.

Such personal data may include, but is not limited to, the following categories

- Supplier Company Name
- Address(es)
- Fax No
- Telephone number(s)
- Email address
- Contact information (first and last name(s), job title(s), email(s), telephone number(s),
- BACS/bank account name, sort code & account number

The information will be retained where there is a legitimate business or legal need to do so. This includes compliance with our legal requirements, dispute resolution,

enforcement of agreements, for other lawful business purpose or in line with statutory requirements.

We use Pegasus Opera 3 / Historical Pegasus Opera System for contract management.

The information is located on a secure domain authenticated network accessed by a unique login password for each member of staff.

This is controlled by our Department Managers, Operations Director & Company Secretary.

8 Data retention

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. See the relevant section in relation to each service we offer for more information about how long we retain personal data for.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

9 Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. These are set out in further detail at the end of this privacy notice.

If you wish to exercise any of these rights, please contact the Data Privacy Manager using the details set out above.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10 **Handling Customers' Personal Data – as part of software support or development**

As part of the software support we provide to our customers, it is sometimes necessary for us to handle our customers' personal data on their behalf, usually but not exclusively for support or development purposes.

Passwords are securely generated using the LastPass application. Password protected access with two-factor authentication. This information is retained whilst the customer remains a customer and deleted if they leave us.

Data files are securely transferred by using one of our approved methods as below:

- LogMeIn — Password protected access
Two-factor authentication
Encrypted
- TeamViewer — Password protected access
Two-factor authentication
Encrypted
- Bomgar — Authenticated client.
User/customer controlled
Secure connection
Encrypted
- WeTransfer — Password protected access
Zipped files are password protected
Our customer acknowledges receipt to our team

Files are available to download by the customer for 7 days and then automatically deleted

Once the spreadsheet has been emailed to us, the password is to then be provided separately to our member of staff whom is dealing with the issue relating to the data (for support, development or other purposes). This can be one of two ways. Firstly, the member of our staff can reply to the customer's email to confirm safe receipt of the spreadsheet/data. The customer can then under separate email then send the password for the document. Secondly, the customer can telephone and speak with our member of staff and provide the password verbally.

For remote access, file transfer as above for Log Me In, TeamViewer and WeTransfer, the access remains whilst the customer is a customer of Davidson Richards Limited and is deleted if they leave.

For Bomgar remote access and file transfer, this is access to the customer's live system and is only available during the dial-in session, under direct customer supervision.

This is controlled by our Operations Director.

Admin & Support

We use Pegasus Opera 3's CRM solution to hold data regarding the customer's system, software development and particular features. In addition, our help desk logs support calls using this system.

We use our in-house designed Staff Time Recording (called RUR) to capture the time spent on a project or activity in 6-minute segments for the purposes of monitoring and billing.

Such personal data may include, but is not limited to, the following categories:

- Customer name
- Activity
- Contact full or first name
- Length of time taken

The above data will be retained where there is a legitimate business or legal need to do so. This includes compliance with our legal requirements, dispute resolution, enforcement of agreements, for other lawful business purpose or in line with statutory requirements.

The information is located on a secure domain authenticated network accessed by a unique login password for each member of staff.

This is controlled by our Operations Director.

Third Party Applications for Customer's Use

OpServices is the name for our web services for our retail solution called OpSuite. OpServices are the gateway to allow 3rd party applications (such as loyalty, financial accounting, ecommerce solutions) to integrate and communicate with our OpSuite retail solution. Such 3rd party applications are defined by the customer.

OpServices are password protected and accessed via a secure encrypted network (https) at UK Fast our hosting partner.

This is controlled by our Operations Director.

Sys Republic is a proprietary protocol software used to transfer data between the HQ & stores for selected retail solutions we provide. This is controlled by our Operations Director.

Email transportation & email defender

We use Inty as our email transportation & email defender software. It is supplied directly to the customers which they access via Microsoft Office 365. We do not access their data, merely act as the agent to sell the software and then providing ongoing software support.

A secure Microsoft admin portal is used to create users and groups.

This is controlled by our Operations Director.

11 Glossary

LAWFUL BASIS

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information

about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

THIRD PARTIES

External Third Parties

- Text Local LTD – we use them to provide our text alert service to alert existing customers on support or system related matters which may affect their business and need urgent attention. Data held includes names, mobile numbers and company details. The data will be retained for as long as you remain a customer and wish to receive the updates.

- LastPass – this is an application generates secure passwords for our software applications software, such as OpServices.

- Log Me In, TeamViewer and Bomgar – we use these for remote access and file transfer for our software applications.

- WeTransfer – used for file transfer of our software applications.

- UK Fast – this hosts our OpSuite retail management and EPoS solution environment.

- Sys Republic – we use this to communicate data between the HQ and stores.

- Professional advisers including lawyers, bankers, auditors and insurers based in the UK who provide consultancy, banking, legal, insurance and accounting services.

- HM Revenue & Customs, regulators and other authorities who require reporting of processing activities in certain circumstances.

YOUR LEGAL RIGHTS

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we

may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.