



Sadler Hair and Beauty
Policies, terms and conditions

Last Updated: April 2020

SALON TERMS AND CONDITIONS

By booking an appointment at Sadler Hair and Beauty you automatically agree to all of the Terms & Conditions listed here.

CANCELLATIONS AND NO SHOWS

Appointments which are cancelled at short notice or clients who fail to show up to their appointment cause inconvenience to other clients, a loss of revenue to the salon and earnings for our hair designers. We therefore ask that you give us **48 hours' notice for any appointment change or cancellation.**

In the event of continuous no show or repeat late cancellations, we may choose to request a 50% non refundable booking fee for future appointments, which will be taken off your bill after service.

Equally, if we have to cancel your appointment we will also endeavour to supply 24 hours' notice. If we are unable to provide 24 hours' notice we will credit the client's account with a discount off the price of the original booking.

LATENESS

If for any reason you are running late for your appointment please call us on 01582 729422

We work very hard to schedule the right amount of time for each service. Accommodating late guests is often impossible without disrupting every other guest scheduled that day. Please be aware in the unfortunate event you are late, we cannot guarantee that your services will be performed that day. Lateness of 10 minutes or more may require rescheduling your appointment for another day.

SERVICE SATISFACTION

If after your appointment you are not satisfied with your service, we ask you to please contact the salon within 7 days of that service. We would like every opportunity to exceed your expectations, as we value you as a client. If you have simply changed your mind or if you return after the 7 days, normal charges will apply. If you have altered or attempted to alter a hair colour or cut yourself or by a third party this guarantee becomes null and void.

SKIN TESTS

If a skin test is required for your colour services and you fail to have one done, then we have no choice but to cancel your appointment. Skin tests must be carried out 48 hours or before your appointment. We insist on following the rules and regulations of the manufacturers that supply our colour for your own safety and well being.

It is very rare for a reaction to occur but if it does it can be very severe and can even cause hospitalisation - this is a risk that we are not willing to take.

COLOUR DIAGNOSTICS AND FORMULAS

Please note, to comply with GDPR, we are not able to give out details of your colour.

GIFT VOUCHERS

Vouchers are valid for a year from purchase and can not be used after that date. Vouchers cannot be replaced if lost, stolen or destroyed. Vouchers cannot be refunded or exchanged for cash or other denominated vouchers.

If an intended purchase is for a higher amount than the face value of the voucher, the difference can be made up with a credit card/cash payment. If it is less, then change cannot be given.

Vouchers cannot be used in conjunction with any special promotions, discount, coupons or cards.

Vouchers cannot be sold to any third parties without our consent. If we do give our consent then such consent may be subject to any conditions which we impose. In any event, you may not sell the Vouchers through the internet without our express written consent, which you must obtain before making any such sale. We reserve the right at all times to refuse to permit any sale of Vouchers by you to a third party.

OFFERS AND PROMOTIONS

We reserve the right to cancel any offer or promotion at any time. Management reserves the right to refuse any service at any time. Services may not be available at all times. All offers, promotions and vouchers may have a minimum spend and are valid for 7 days from day offer/voucher is sent unless otherwise stated. These cannot be redeemed for cash or used in conjunction with any other offer, discount or promotion. One voucher per person per visit. Unless otherwise stated all offers, vouchers, discounts and promotions exclude Children and Gents appointments. Some promotions require payment before the appointment can be booked - this payment is non-refundable if you fail to turn up or change the appointment without 48 hours notice.

PERSONAL BELONGINGS

The company will not accept any responsibility for the loss or damage (including clothing) to any personal belongings that you bring to the salon with you.

While the team will always endeavour to keep your personal belongings safe and undamaged we cannot accept any responsibility for loss or damage of your personal possessions while on the premises. We do take every precaution possible to protect your clothes from colour but we would advise you to wear something appropriate to avoid disappointment. High necklines and collars are best avoided. We highly recommended not to wear expensive clothing while getting your hair coloured at the salon.

DOGS

We are very happy to welcome well behaved dogs into the salon.

DATA PROCESSING NOTICE

WHEREAS: (A) The Company acts as a Data Controller. (B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor. (C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation 1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules; 1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement; 1.1.3 "Contracted Processor" means a Subprocessor;

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country; 1.1.5 "EEA" means the European Economic Area; 1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR; 1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679; 1.1.8 "Data Transfer" means: 1.1.8.1 a transfer of

Company Personal Data from the Company to a Contracted Processor; or 1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws); 1.1.9 "Services" means the _____ services the Company provides. 1.1.10 "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement. 1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly. 2. Processing of Company Personal Data 2.1 Processor shall: 2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and 2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data. 3. Processor Personnel Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. 4. Security 4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. 4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach. 5. Subprocessing 5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company. 6. Data Subject Rights 6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws. 6.2 Processor shall: 6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and 6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws

inform Company of that legal requirement before the Contracted Processor responds to the request. 7. Personal Data Breach 7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach

affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. 7.2 Processor shall cooperate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach. 8. Data Protection Impact Assessment and Prior Consultation Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors. 9. Deletion or return of Company Personal Data 9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data. 9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date. 10. Audit rights 10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors. 10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer 11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data. 12. General Terms 12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that: (a) disclosure is required by law; (b) the relevant information is already in the public domain. 12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction 13.1 This Agreement is governed by the laws of the England and Wales.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of England and Wales, subject to possible appeal

PRIVACY NOTICE

INTRODUCTION

Kiss Curl 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.

You can download a pdf version of the notice *here*. Please also use the Glossary at the end of this privacy notice to understand the meaning of some of the terms used in it.

1. IMPORTANT INFORMATION AND WHO WE ARE

PURPOSE OF THIS PRIVACY NOTICE

This privacy notice aims to give you information on how we collect and process the personal data you provide when you:

- visit our websites (regardless of where you visit it from);
- make an order from our online shop;
- sign up to the Sadler newsletter; or
- take part in a competition or prize draw

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

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

CONTROLLER

Kiss Curl Limited are the data controller and responsible for your personal data (collectively referred to as “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 data privacy manager using the details set out below.

CONTACT US

Our full details are:

Full name of legal entity: Kiss Curl Limited

FAO: Data Privacy Manager

Email address: dataprotection@sadlerhairandbeauty.com

Postal address: 20 Stuart Street, Luton, Bedfordshire. LU1 2SL

Telephone number: 01582 729 422

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.

CHANGES TO THE PRIVACY NOTICE AND YOUR DUTY TO INFORM US OF CHANGES

This version was last updated on 20 April 2020.

We reserve the right to amend this Privacy Notice at any time. Any changes we may make to our notice in the future will be posted on this page and, where appropriate, notified to you by email or SMS.

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 and periodically review your account with us if you have one.

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:

- **Identity Data** – includes first name, last name, username or similar identifier, title, date of birth, gender and images of you if you entered the label-me competition.
- **Contact Data** – includes billing address, delivery address, email address, telephone numbers or any other data you provide to enable us to contact you.
- **Transaction Data** includes details about payments to and from you and other details of products and services you have purchased from us.

- **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.
- **Profile Data** includes your username and password, purchases or orders made by you, points on your rewards card, preferences, feedback and survey responses.
- **Usage Data** includes information about how you use our website, products and services.
- **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. Nor do we collect any information about criminal convictions and offences.

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, Transaction and Profile by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
 - purchase our products or services;
 - 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. We may also receive Technical Data about you if you visit other websites employing our cookies.

- **Third parties.** We may receive personal data about you from various third parties as set out below:
 - Contact, Transaction, Technical and Usage Data from analytics providers such as Google;
 - Identity, Contact, Technical, Profile and Transaction Data from providers of technical, payment, feedback and delivery services;
 - Contact, Transaction, Technical and Usage Data from advertising networks.

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 to send marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us using the details above.

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 using the details above 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 and Types of Data Used | Lawful basis for processing including basis of legitimate interest |
|--|---|
| To register you as a new customer <i>Data: Identity, Contact and Allergy Test</i> | Performance of a contract with you |

| | |
|---|--|
| <p>To provide you with your order or service which includes:</p> <p>(a) Manage payments, fees and charges</p> <p>(b) Collect and recover money owed to us</p> <p>Data: <i>Identity, Contact, Allergy Test, Profile and Transaction</i></p> | <p>(a) Performance of a contract with you</p> <p>(b) Necessary for our legitimate interests (to recover debts due to us)</p> <p>(c) Necessary for your legitimate interests (to ensure that we provide you with a safe service)</p> |
| <p>To manage our relationship with you which will include:</p> <p>(a) Notifying you about changes to our terms or privacy notice</p> <p>(b) Asking you to leave a review or take a survey</p> <p>Data: <i>Identity, Contact, Profile, Transaction and Marketing and Communications</i></p> | <p>(a) Performance of a contract with you</p> <p>(b) Necessary to comply with a legal obligation</p> <p>(c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)</p> |
| <p>To enable you to partake in a prize draw, competition or complete a survey</p> <p>Data: <i>Identity, Contact, Profile, Usage and Marketing and Communications</i></p> | <p>(a) Performance of a contract with you</p> <p>(b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)</p> |
| <p>To administer and protect our business and website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)</p> <p>Data: <i>Identity, Contact and Technical</i></p> | <p>(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)</p> <p>(b) Necessary to comply with a legal obligation</p> |
| <p>To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you</p> | <p>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)</p> |

| | |
|--|---|
| <i>Data: Identity, Contact, Profile, Usage, Marketing and Communications, Technical</i> | |
| To use data analytics to improve our website, products/services, marketing, customer relationships and experiences <i>Data: Technical, Usage and Profile</i> | 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 <i>Data: Identity, Contact, Usage, Technical and Profile</i> | Necessary for our legitimate interests (to develop our products/services and grow our business) |

MARKETING AND 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.

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

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. To stop receiving any marketing communications from us, please follow the instructions in the 'Opting out' section below.

THIRD-PARTY MARKETING

We will never share your personal data with any third parties for marketing purposes.

OPTING OUT

- If you have an account with us you can update your marketing preferences
- To stop receiving marketing communications by email please follow the unsubscribe link at the bottom of every email
- Contact us on the details above

Please note that you may still receive some marketing messages for a short period after you have updated your marketing preferences, while our systems are fully updated. After that, please note that you will still receive information and service updates.

COOKIES

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

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 using the details above.

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 AND THIRD PARTIES

We may also collect from and share your personal data with the parties set out below for the purposes set out in the table in paragraph 4 above.

- Internal Third Parties as set out in the *Glossary*.
- 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.

6. INTERNATIONAL TRANSFERS

We do not transfer 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. 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 will notify you and any applicable regulator of a breach where we are legally required to do so.

8. DATA RETENTION

HOW LONG WILL YOU USE MY PERSONAL DATA FOR?

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.

Details of retention periods for different aspects of your personal data are as follows:

- If you open an online account with us and order products, we will retain your personal data for as long as necessary to comply with our legal and contractual obligations. If you choose to delete your online account, you should be aware that some data will be retained to comply with our legal obligations and legitimate business interests.
- If you have subscribed to our newsletter, your personal data will be held for as long as you remain a subscriber to the newsletter. If you choose to unsubscribe, then we will hold the record of your unsubscribe request to ensure that we comply with our legal obligations.

In some circumstances you can ask us to delete your data: see Your Legal Rights below for further information.

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 the following rights under data protection laws in relation to your personal data (further details of which are contained in the Glossary) to:

- **request access** to your personal data
- **request correction** of your personal data
- **request erasure** of your personal data
- **object to processing** of your personal data
- **request restriction of processing** your personal data
- **request transfer** of your personal data
- **withdraw consent**

If you have an online account with us, then you can click on the 'my details' section of the website to access and update the information we hold at any time should this need updating.

If you wish to make a complaint or you wish to exercise any of the rights set out above, please Contact us using the details 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. 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 using the above details.

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

INTERNAL THIRD PARTIES

Group companies acting as joint controllers or processors and who are based in the United Kingdom and provide IT and system administration services and undertake leadership reporting.

EXTERNAL THIRD PARTIES

- Service providers acting as processors for example delivery services, cloud storage providers and IT and system administration providers
- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers based in the United Kingdom who provide consultancy, banking, legal, insurance and accounting services
- HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of processing activities in certain circumstances
- Analytics providers who provide analytics tools to track the way users interact with our website
- Email service providers and marketing platforms to provide marketing materials to you
- Payment providers who facilitate payments made on our website
- Feedback providers: when you make a purchase, we engage a third party to send out feedback forms on our behalf

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.

CCTV PRIVACY NOTICE

CCTV Policy

At Sadler we believe that CCTV plays a legitimate role in helping to maintain a safe and secure environment for all our staff, guests, customers, and potential customers, tenants, employees of its partners and suppliers and contractors .

Images recorded by CCTV are Personal Data and as such must be processed in accordance with data protection laws. We are committed to complying with our legal obligations in order to appropriately handle and protect Personal Data and ensure that the legal rights of staff, guests, customers, and potential customers, tenants, employees of its partners and suppliers and contractors relating to their Personal Data, are recognised and respected.

This policy is intended to enable staff, guests, customers, and potential customers, tenants, employees of its partners and suppliers and contractors to understand how Sadler uses CCTV, those departments responsible for CCTV use, the rights individuals may have in relation to CCTV, who has access to CCTV images and how individuals can raise any queries or concerns they may have.

1. Definitions

For the purposes of this policy, the following terms have the following meanings:

CCTV: means cameras, devices or systems including fixed CCTV and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

CCTV Data: means any Data in respect of CCTV, e.g. video images, static pictures, etc.

Data: means any information which is stored electronically or in paper-based filing systems.

Data Subject: means any individuals who can be identified directly or indirectly from CCTV Data (or other Data in our possession). Data Subjects include staff, guests, customers, and potential customers, tenants, employees of its partners, suppliers and contractors, and members of the public.

Data Controller: is the organisation or authority which, determines how and for what purpose the Personal Data are processed. When operating CCTV, Sadler is the relevant Data Controller and is responsible for ensuring compliance with the Data Protection Laws.

CCTV users: are those of our employees (or employees of any Data Processors which we appoint) whose work involves processing CCTV Data. This will include those whose duties are to operate CCTV to record, monitor, store, retrieve and delete images. Data users must protect the CCTV Data they handle in accordance with this policy.

Service Provider: is any organisation that is not a CCTV user (or other employee of a Data Controller) that processes CCTV Data or Personal Data on our behalf and in accordance with our instructions (for example, Choice Fire and Security Solution).

Data Protection Laws: means:

a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data (General Data Protection Regulation) (the “GDPR”) and any equivalent or implementing legislation;

b) all other applicable laws, regulations or court judgements relating to the processing of personal data, data privacy, electronic communications, marketing and/or data security; and

c) any and all legally binding guidelines, recommendations, best practice, opinions, directions, decisions, or codes issued, adopted or approved by the European Commission, the Article 29 Working Party, the European Data Protection Board, the UK’s Information Commissioner’s Office and/or any other supervisory authority or data protection authority from time to time in relation to the processing of personal data, data privacy, electronic communications, marketing and/or data security;

in each case as from time to time in force and as from time to time amended, extended, consolidated, re-enacted, replaced, superseded or in any other way incorporated into law and all orders, regulations, statutes, instruments and/or other subordinate legislation (including the Data Protection Bill 2017 when in force) made under any of the above in any jurisdiction from time to time.

Processing: is any activity which involves the use of CCTV Data, whether or not by automated means. It includes collecting, obtaining, recording or holding CCTV Data, or carrying out any operation or set of operations on the CCTV Data including organising, structuring, amending, retrieving, using, disclosing or erasing or destroying it. Processing also includes transferring CCTV Data to third parties.

Site: means the Sadler premises at Sadler, Chichester Street, London, SW1V 3LX and more specifically the Sites listed in Schedule 1 where CCTV is installed.

2. About this policy

2.1: We currently use CCTV to view and record individuals at our Site, 24 hours per day, 7 days per week. This policy sets out why we use CCTV, how we will use CCTV and how we will process any CCTV Data recorded by CCTV to ensure that we are compliant with Data Protection Law.

2.2: The images of individuals recorded by CCTV are Personal Data and therefore subject to the Data Protection Laws. Sadler is the Data Controller of all CCTV Data captured at our Site.

2.3: This policy covers all staff, guests, customers, and potential customers, tenants, employees of its partners and suppliers and contractors and may also be relevant to members of the public visiting the Site.

3. Staff responsible

Sadler, Head of Security has overall responsibility for ensuring compliance with Data Protection Laws and the effective operation of this policy. Day-to-day operational responsibility for CCTV and the storage of CCTV Data recorded is the responsibility of the Duty Security Controller. Should you have any queries on the use of CCTV or surveillance systems by us please contact Sadler, Head of Security.

4. Why we use CCTV

4.1: We currently use CCTV around our Site as outlined below. We believe that such use is necessary for the following legitimate business purposes:

- (a) to prevent or detect crime and protect buildings and assets from damage, disruption, theft, vandalism and other crime;
 - (b) for the personal safety of staff, guests, customers, and potential customers, tenants, employees of its partners, suppliers and contractors and other members of the public and to act as a deterrent against crime;
 - (c) for health and safety of those using the pool and gym floor;
 - (d) to support law enforcement bodies in the prevention, detection and prosecution of crime; and
 - (e) to support any internal investigations as part of a staff disciplinary procedure.
- We may implement or use CCTV for purposes other than those specified above which we will notify you of from time to time.

5. MONITORING

5.1: The locations of the CCTV are chosen to minimise the viewing of spaces/individuals which are not relevant to the legitimate purpose of the monitoring as specified above.

5.2: Currently, none of our CCTV records sound.

5.3: A live feed from the CCTV is not monitored continuously and images are only revisited in the event of an incident or if a request is made.

5.4: Any staff using CCTV will be given training to ensure that they understand and observe the legal requirements relating to the processing of any Data gathered.

6. How we operate CCTV

6.1: Where CCTV is in use at our Site, we will ensure that signs are displayed at the entrance of the surveillance zone to alert staff, guests, customers, and potential customers, tenants, employees of its partners, suppliers and contractors that their image may be recorded. The signs will contain details of the organisation operating the system (where they are operated by a third party) and who to contact for further information.

6.2: We will ensure that live feeds from the CCTV are only viewed by appropriately authorised members of staff or third-party service providers whose role requires them to have access to such CCTV Data. Recorded images will only ever be viewed in the Security Manager's Office or the General Manager's Office which are secure and restricted areas by our security staff, departments managers, the General Manager or the Health and Safety Manager.

7. How we use the Data

7.1: In order to ensure that the rights of individuals recorded by our CCTV are protected, we will ensure that CCTV Data gathered from such systems is stored in a way that maintains its integrity and security. This may include encrypting the Data, where it is possible to do so.

7.2: We will ensure that any CCTV Data is only used for the purposes specified in section 4.1 above. We will not use CCTV Data for another purpose unless permitted by Data Protection Laws.

7.3: Where we engage Data Processors to process Data on our behalf, we will

ensure contractual safeguards are in place to protect the security and integrity of the Data.

8. Retention and erasure of Data

8.1: Data recorded by our CCTV will be stored locally on servers at our Site. We will not retain this Data indefinitely but will permanently delete it once there is no reason to retain the recorded information. Exactly how long the Data will be retained for will vary according to the purpose for which it was recorded. For example, where images are being recorded for crime prevention purposes, CCTV Data will be kept only for as long as it takes to establish that a crime has been committed or where we are using the CCTV Data for staff disciplinary purposes, the images will be kept until the process is completed. In all other cases, recorded images will be kept for no longer than 30 days before being overwritten and permanently deleted.

8.2: At the end of its useful life and in any event within 7 years all Data stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs or hard copy photographs will be promptly disposed of as confidential waste.

9 Ongoing review of our use of CCTV

9.1: We will periodically review our ongoing use of existing CCTV at our Site to ensure that its use remains necessary and appropriate and in compliance with Data Protection Laws.

9.2: We will also carry out checks to ensure that this policy is being followed by all staff.

10. Rights of Data Subjects

10.1 As CCTV Data will identify individuals, it will be considered Personal Data under applicable Data Protection Laws. Under Data Protection Laws, Data Subjects have certain rights in relation to the Personal Data concerning them. These are as follows:

(a) the right to access a copy of that Personal Data and the following information (this may include CCTV Data captured by our CCTV):

(i) the purpose of the processing;

(ii) the types of Personal Data concerned;

(iii) to whom the Personal Data has or will be disclosed; and

(iv) the envisaged period that the Personal Data will be stored, or if not possible, the criteria used to decide that period;

(b) the right to request any inaccurate Personal Data that we hold concerning them is rectified, this includes having incomplete Personal Data completed;

(c) the right to request the Personal Data we hold concerning them is erased without undue delay, where it is no longer necessary for us to retain it in relation to the purposes it was collected;

(d) the right to request restriction of our processing of Personal Data in certain circumstances; and

(e) the right to lodge a complaint with the Information Commissioner's Office, if the Data Subject considers that our processing of the Personal Data relating to him or her infringes Data Protection Laws.

11. SERVICE PROVIDERS

11.1 In order to operate CCTV across our Site we appoint service providers to provide us with maintenance services related to that CCTV. Such service providers act only on our instructions and on our behalf for the purposes listed in section 4.1 above. We require these service providers by contract to safeguard the privacy and security of Personal Data they process on our behalf.

12. Requests of disclosure by third parties

12.1: No images from our CCTV cameras will be disclosed to any third party, without express permission being given by The General Manager. Data will only be disclosed to a third party in accordance with Data Protection Laws.

12.2: In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

13. Complaints

13.1: If any person has questions about this policy or any concerns about our use of CCTV, then they should contact us.

13.2: Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure. If you are not an employee, you can use our official complaints procedure.