Data Protection Policy

Table of Contents

1. Introduction

1.1 North Ayrshire Leisure Limited ("**KAL**") hold personal data about our staff, clients, suppliers and other individuals for a variety of Business Purposes.

1.2 This policy sets out how KAL complies with our data protection obligations and seeks to protect personal data. Its purpose is also to ensure that all KAL personnel understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their work.

1.3 KAL is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations including, without limitation, under the Data Protection Laws. KAL is also committed to being concise, clear and transparent about how KAL obtains and uses personal data relating to our business, and how (and when) KAL deletes that information once it is no longer required.

1.4 The Data Protection Officer is responsible for informing and advising KAL and its personnel on its data protection obligations, and for monitoring compliance with those obligations and with KAL's policies related to data protection. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Data Protection Officer.

2. Scope

2.1 This policy applies to all KAL personnel, who must be familiar with this policy and comply with its terms.

2.2 References to KAL personnel or person include all employees, directors, officers, consultants, contractors, casual workers, agency workers and anyone who has access to KAL premises or systems.

2.3 This policy supplements our other policies relating to internet and email use. This policy does not form part of any employee's contract of employment and KAL may supplement or amend this policy at any time.

3. Definitions

Business Purposes — means the purposes for which personal data may be used by us:

Personnel, administrative, financial, regulatory, payroll and benefits and business purposes.

Business purposes include the following:

- To provide leisure services and other services to clients, including gym membership and facility hire;
- To ensure the confidentiality of commercially sensitive information;
- To manage and administer our business relationship with clients and other third parties, including use for the purposes of processing payments, accounting, auditing, billing and collection and other support services;
- To deal with any complaints received;
- To ensure business policies are adhered to, e.g. policies covering security and internet use and to prevent unauthorised access and modifications to systems;
- For operational reasons, such as ensuring safe working practices, improving efficiency, risk management, training, personnel assessment and quality control;
- For statistical analysis to help us improve our services and communications within and out with KAL or to evaluate the strength of our relationship with clients and relevant third parties;
- Updating and enhancing client records;
- For marketing our services;
- For the purposes of external audits and quality checks, e.g. for Investors in People accreditation and the audit of our accounts;

- For insurance purposes;
- To complete statutory returns;
- To identify those who are authorised to deal with KAL on behalf of our clients, suppliers and/or service providers;
- For recruitment purposes;
- Processing personal data which is provided to us by or on behalf of our clients for the purposes of services we provide to them;
- To allow us to pay personnel and provide personnel with benefits (including liaising with pension providers) and making related tax and National Insurance contributions;
- Business management and planning, including accounting, auditing, equal opportunities monitoring, and to conduct employment data analytics studies; and/or
- Managing performance, salary reviews and compensation decisions, assessing training and development requirements, and making promotion decisions.

Data controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	means a natural or legal person, agency or other body which processes personal data on behalf of the controller.
Data Protection Laws	means all applicable legislation and regulations relating to the processing of personal data and privacy including (without limitation) the Data Protection Act 2018, the GDPR as the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Data Protection (Processing of Sensitive Personal Data) Order 2000 or any amendments and/or re-enactments of any of the same together with any regulations or instruments enacted under any of the foregoing.
GDPR	means Regulation (EU) 2016/679 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).
Personal data	means any information relating to an identified or identifiable natural person ("**data subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4. The principles

KAL shall comply with the principles of data protection (the "**Principles**") set out in the GDPR. KAL will make every effort possible in everything KAL does to comply with these Principles. The Principles are:

4.1 **Lawful, fair and transparent:** Data collection must be fair, for a legal purpose and KAL must be open and transparent as to how the data will be used.

4.2 **Limited for its purpose:** Data can only be collected for a specific purpose.

4.3 **Data minimisation:** Any data collected must be necessary and not excessive for its purpose.

4.4 **Accurate:** The data KAL holds must be accurate and kept up to date.

4.5 **Retention:** KAL cannot store data longer than necessary.

4.6 **Integrity and confidentiality:** The data KAL holds must be kept safe and secure.

5. Accountability and transparency

5.1 To comply with Data Protection Laws and the accountability and transparency principle of the GDPR, KAL must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure KAL meets the following data protection obligations:

5.1.1 Fully implementing all appropriate technical and organisational measures;

5.1.2 Maintaining up to date and relevant documentation on all processing activities;

5.1.3 Conducting data protection impact assessments ("**DPIAs**");

5.1.4 Implementing measures to ensure privacy by design and default, including:

(i) Data minimisation;

(ii) Pseudonymisation;

(iii) Transparency;

(iv) Allowing individuals to monitor processing;

(v) Creating and improving security and enhanced privacy procedures on an ongoing basis.

5.2 KAL is classified as a data controller and in some circumstances we may also act as a data processor. KAL must maintain an appropriate registration with the Information Commissioner's Office in order to continue lawfully controlling and/or processing data.

5.3 Where KAL is providing services to customers it is acting as data controller as it is determining the purposes for which the personal data is processed for the purposes of providing the services.

5.4 Where we act as a data processor, KAL must comply with our contractual obligations and act only on the documented instructions of the data controller (unless they are unlawful).

5.5 If you are in any doubt about how KAL handles data, contact the Data Protection Officer for clarification.

6. Lawful basis for processing personal data

6.1 In relation to any processing activity KAL will, before the processing starts for the first time, and then regularly while it continues:

6.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(i) that the data subject has consented to the processing;

(ii) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(iii) that the processing is necessary for compliance with a legal obligation to which KAL is subject;

(iv) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; *or*

(v) that the processing is necessary for the purposes of legitimate interests of KAL or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject - see paragraph 6.4 below;

6.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

6.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the Principles;

6.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

6.1.5 where special categories of personal data are processed, also identify a lawful special condition for processing that information (see paragraph 7.2.2 below), and document it; and

6.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

6.2 Where KAL is making an assessment of the lawful basis, it must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. KAL cannot rely on a lawful basis if we can reasonably achieve the same purpose by some other means.

6.3 More than one basis may apply, and KAL will rely on what will best fit the purpose, not what is easiest. In carrying out our assessment, KAL will consider a number of factors and will document the answers.

6.4 When determining whether KAL's legitimate interests are the most appropriate basis for lawful processing, KAL will:

6.4.1 conduct a legitimate interests assessment ("**LIA**") and keep a record of it, to ensure that KAL can justify our decision;

6.4.2 if the LIA identifies a significant privacy impact, consider whether KAL also needs to conduct a DPIA;

6.4.3 keep the LIA under review, and repeat it if circumstances change; and

6.4.4 include information about our legitimate interests in our relevant privacy notice(s).

6.5 KAL must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether KAL has collected the data directly from the individual, or from another source.

6.6 Before carrying out any new forms of processing of personal data, you must notify the Data Protection Officer of the proposed processing and discuss and agree responsibilities for ensuring that the proposed processing complies with the criteria noted above.

7. Special categories of personal data

7.1 Previously known as sensitive personal data, special categories of personal data means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

7.1.1 race;

7.1.2 ethnic origin;

7.1.3 politics;

7.1.4 religion;

7.1.5 trade union membership;

7.1.6 genetics;

7.1.7 biometrics (where used for ID purposes);

7.1.8 health;

7.1.9 sexual orientation.

7.2 KAL may from time to time need to process special category personal data. KAL will only process such special category personal data if:

7.2.1 KAL has a lawful basis for doing so as set out in paragraph 6.1.1 above, e.g. it is necessary for the performance of the employment contract, to comply with KAL's legal obligations or for the purposes of KAL's legitimate interests; and

7.2.2 one of the special conditions for processing such special category personal data applies, e.g.:

(i) the data subject has given explicit consent;

(ii) the processing is necessary for the purposes of exercising the employment law rights or obligations of KAL or the data subject;

(iii) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(iv) processing relates to personal data which are manifestly made public by the data subject;

(v) processing is necessary for the establishment, exercise or defence of legal claims; or

(vi) processing is necessary for reasons of substantial public interest.

7.3 Special category personal data will not be processed until:

7.3.1 (where the processing is a new form of processing), a discussion as referred to in paragraph 7.7 has taken place and an appropriate assessment has been undertaken; and

7.3.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

7.4 KAL will not carry out automated decision-making (including profiling) based on any individual's personal data which falls within the special categories.

7.5 If KAL processes special category personal data or criminal records information, KAL will keep written records of:

7.5.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

7.5.2 the lawful basis for our processing; and

7.5.3 whether KAL retains and erases the personal data.

7.6 KAL has a data protection privacy notice which relates to processing of personnel data and data protection privacy notices that relates to all other forms of processing carried out by KAL. These notices set out the types of special category personal data that KAL processes, what it is used for and the lawful basis for the processing.

7.7 Before carrying out any new forms of processing of special category personal data, you must notify the Data Protection Officer of the proposed processing and discuss and agree responsibilities with them for ensuring that the proposed processing complies with the criteria noted above.

8. Criminal records information

Any criminal record checks must be justified by law. Criminal record checks cannot be undertaken based solely on the consent of the data subject. KAL cannot keep a comprehensive register of criminal offence data. You must have approval from the Data Protection Officer prior to carrying out a criminal record check. Criminal records information will be processed in accordance with our procedure for employment of personnel (Vetting) – HMG requirements.

9. Privacy notices

9.1 KAL must supply a privacy notice at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, KAL must provide the privacy notice within a reasonable period of having obtained the data, ideally within one month. Our Privacy Policy which is available at www.kaleisure.com and therefore issuing a letter of engagement to a client will deal with bringing this information to their attention. If you have further

questions about whether or not you have complied with this clause 9.1 you should contact the Data Protection Officer.

9.2 If the data is being used to communicate with the individual, KAL must supply the privacy notice at the latest when the first communication takes place.

9.3 If disclosure to another recipient is envisaged, KAL must supply the privacy notice prior to the data being disclosed.

9.4 Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language.

10. Accuracy and relevance

10.1 KAL will ensure that any personal data KAL processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. KAL will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

10.2 Individuals may ask that KAL corrects inaccurate or incomplete personal data relating to them. Further detail on this is provided in paragraph 11 below and in our Individuals' Rights Policy.

11. Individuals' rights

11.1 Data subjects have the following rights in relation to their personal data:

11.1.1 to be informed about how, why and on what basis that information is processed – this will usually be done by way of a privacy notice;

11.1.2 to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request;

11.1.3 to have data corrected if it is inaccurate or incomplete;

11.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

11.1.5 to restrict the processing of personal data where the accuracy of the information is contested, or the processing is unlawful (but the data subject does not want the data to be erased), or where KAL no longer needs the personal data but the information is required to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal data temporarily where the data subject does not think it is accurate (and KAL is verifying whether it is accurate), or where the data subject has objected to the processing (and KAL is considering whether we have legitimate grounds to override the data subject's interests).

11.2 A data subject has the right to be provided with a copy of their personal data in a format which means they can reuse it for their own purposes or across different services. This means that KAL must provide it in a commonly used, machine-readable format. This would normally be a CSV file, although other formats are acceptable. KAL must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to.

11.3 A data subject has the right to object to:

11.3.1 data processing based on legitimate interests or the performance of a public interest task;

11.3.2 direct marketing, including profiling;

11.3.3 processing of their data for scientific and historical research and statistical purposes,

and in each case KAL must take account of such objection as appropriate.

11.4 KAL must respect the rights of individuals in relation to automated decision making and profiling. Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

11.5 If a data subject wishes to exercise any of the rights in paragraphs 11.1.2 to 11.1.6 or 11.4, please ask them to contact the Data Protection Officer.

12. Subject access requests

12.1 If you believe that you have received a request for a copy of personal data you must **immediately pass this to the Data Protection Officer. You should not in any circumstances attempt to respond to the subject access request yourself.** It is important that the Data Protection Officer is notified immediately because of the timescales for responding to such a request which are set out below.

12.2 KAL must provide an individual with a copy of the personal data covered by the request, free of charge. This must occur without delay, and within one month of receipt. KAL will endeavour to provide data subjects access to their information in commonly used electronic formats. KAL will follow the procedure set out in our Individuals' Rights Policy.

12.3 If complying with the request is complex or involves dealing with numerous requests, the deadline can be extended by two months, but the individual must be informed within one month. The Data Protection Officer must approve any extension of the deadline.

12.4 KAL can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, KAL can request the individual specify the information they are requesting. This can only be done with express permission from the Data Protection Officer.

12.5 **Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.**

13. Data protection impact assessments ("**DPIAs**")

13.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where KAL is planning to use a new form of technology), KAL will, before commencing the processing, carry out a DPIA to assess:

13.1.1 whether the processing is necessary and proportionate in relation to its purpose;

13.1.2 the risks to individuals; and

13.1.3 what measures can be put in place to address those risks and protect personal data.

13.2 Before any new form of technology is introduced, the Partner/Management Services Director responsible should therefore contact the Data Protection Officer in order that a DPIA can be carried out.

14. Documentation and records

14.1 Where KAL uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. In particular, contracts with external organisations must provide that:

14.1.1 the organisation may act only on the written instructions of KAL;

14.1.2 those processing the data are subject to a duty of confidentiality;

14.1.3 appropriate measures are taken to ensure the security of processing;

14.1.4 sub-contractors are only engaged with the prior consent of KAL and under a written contract;

14.1.5 the organisation will assist KAL in providing subject access and allowing individuals to exercise their rights in relation to data protection;

14.1.6 the organisation will assist KAL in meeting its obligations in relation to the security of processing, the notification of data breaches and DPIAs;

14.1.7 the organisation will delete or return all personal data to KAL as requested at the end of the contract; and

14.1.8 the organisation will submit to audits and inspections, provide KAL with whatever information it needs to ensure that they are both meeting their data protection

obligations, and tell KAL immediately if it is asked to do something infringing Data Protection Laws.

14.2 Before any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is altered, the relevant personnel must seek approval of its terms from our Data Protection Officer.

14.3 KAL will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve special category personal data or criminal records information.

14.4 KAL will conduct regular reviews of the personal data KAL processes and will update our documentation accordingly. This may include:

14.4.1 carrying out information audits to find out what personal data KAL holds;

14.4.2 distributing questionnaires and talking to personnel across KAL to get a more complete picture of our processing activities; and

14.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

14.5 KAL documents our processing activities in electronic form so KAL can add, remove and amend information easily.

15. Individual obligations

15.1 KAL personnel are responsible for helping KAL keep their personal data up to date. You should let the HR department know if the personal information you have provided to KAL changes, for example if you move house or change details of the bank or building society account to which you are paid. Alternatively, those with access to KA Gateway can update their own personal data by downloading and completing the appropriate forms.

15.2 In the course of your employment or engagement you may have access to the personal data of other KAL personnel, suppliers and clients of KAL. If so, KAL expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 11 above.

15.3 If you have access to personal data, you must:

15.3.1 only access the personal data that you have authority to access, and only for authorised purposes;

15.3.2 only allow other KAL personnel to access personal data if they have appropriate authorisation;

15.3.3 only allow individuals who are not KAL personnel to access personal data if you have specific authority to do so from the Data Protection Officer;

15.3.4 keep personal data secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in our ICT Acceptable Use Policy);

15.3.5 not remove personal data, or devices containing personal data (or which can be used to access it), from KAL's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

15.3.6 not store personal data on local drives or on devices that are used for non-work purposes.

16. Information security

KAL will use appropriate technical and organisational measures in accordance with our ICT Acceptable Use Policy to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

17. Storage and retention of personal data

17.1 Personal data (and special category personal data) will be kept securely in accordance with our Data Protection and Privacy Policies.

17.2 Personal data (and special category personal data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. Personnel should follow our Records Management Policy which sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, personnel should consult the Data Protection Officer.

17.3 Personal data (and special category personal data) that is no longer required in terms of our Records Management Policy will be permanently deleted from our information systems and any hard copies will be destroyed securely.

18. Data breaches

18.1 You must report any breach of this policy or of the Data Protection Laws as soon as you have become aware of a breach to the Data Protection Officer. KAL has a legal obligation to report notifiable data breaches to the Information Commissioner's Office within **72 hours**.

18.2 Any KAL person who fails to notify a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures, will be liable to disciplinary action.

19. International transfers

KAL may transfer personal data outside the European Union to third party countries. Where KAL makes such transfers it shall only be done in accordance with one of the basis for processing set out in Chapter V of the GDPR. If you believe that you are going to be transferring personal data outside the European Union then you must contact the Data Protection Officer prior to such transfer.

20. Training

20.1 KAL will ensure that personnel are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

20.2 You will receive adequate training on provisions of Data Protection Laws specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities. If you require additional training on data protection matters contact the Data Protection Officer.

21. Consequences of failing to comply

21.1 KAL takes compliance with this policy very seriously. Failure to comply with this policy:

21.1.1 puts at risk the individuals whose personal data is being processed; and

21.1.2 carries the risk of significant civil and criminal sanctions for the individual and KAL; and

21.1.3 may, in some circumstances, amount to a criminal offence by the individual.

21.2 Everyone must observe this policy. You must notify the Data Protection Officer of any breaches of this policy. You must comply with this policy fully and at all times.

21.3 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract or access to premises or systems terminated with immediate effect.

22. Other relevant areas of risk and compliance

22.1 This policy should be read in conjunction with other KAL policies, including in particular:

22.1.1 ICT Acceptable Use Policy; and

22.1.2 Code of Conduct

23. Queries and feedback

23.1 Any queries in connection with this policy should be directed to the Data Protection Officer.

23.2 Any comments or feedback on the content of this policy should be submitted in writing to the Data Protection Officer, KA Leisure Head Office, 22 Quarry Road, Irvine KA12 0TH. Or by email to: dataprotectionofficer@kaleisure.com