Clancy Briggs Limited (trading as Clancy Briggs Cycling Academy) General Data Protection Regulations Policy (GDPR and DPA 2018) (UK).

This policy can also be found on our website *www.clancybriggs.co.uk*

Version 1.0 September 2019

CONTENTS

CLAUSE

ANNEX

Clancy Briggs Limited (trading as Clancy Briggs Cycling Academy) provides a range of activities to children, young people and their families at different venues across the region. Ensuring that it looks after and keeps safe the data it holds on employees, service users (and their representatives) and partner organisations is paramount. This policy has been developed taking into account the requirements of the General Data Protection Regulations which were issued in May 2018 and will be kept up to date as legislation changes.

1. ABOUT THIS POLICY

1.1 The corporate information, records and data of Clancy Briggs Limited is important to how we conduct business and manage employees.

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

1.3 This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. SCOPE OF POLICY

2.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

2.2 This policy also covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices.

2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

2.4 This policy applies to all aspects of the services provided by Clancy Briggs Limited (trading as Clancy Briggs Cycling Academy).

3. GUIDING PRINCIPLES

3.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

4. ROLES AND RESPONSIBILITIES

4.1 **Responsibility of all employees**. We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices.

4.2 All employees must comply with this policy, the Record Retention Schedule, any communications suspending data disposal and any specific instructions from the Data Protection Officer or Directors of the Company.

4.3 Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

4.4 **The Directors of the Company** are responsible for identifying the data that we must or should retain, and determining, the proper period of retention. It also arranges for the proper storage and retrieval of data, co-ordinating with outside vendors where appropriate.

4.5 We have designated Sam Briggs, **as the Data Protection Officer.**

4.6 Our Data Protection Officer (DPO) is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data.

5. TYPES OF DATA AND DATA CLASSIFICATIONS

5.1 **Formal or official records.** Certain data is more important to us and is, therefore, listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see paragraph 6.1 below for more information on retention periods for this type of data.

5.2 **Disposable information**. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the Clancy Briggs Cycling Academy and retained primarily for reference purposes.
- Spam and junk mail.

Please see paragraph 6.2 below for more information on how to determine retention periods for this type of data.

5.3 **Personal data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). See paragraph 6.3 below for more information on this.

5.4 **Confidential information belonging to others**. Any confidential information that an employee may have obtained from a source outside of the Clancy Briggs Cycling Academy, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

5.5 **Data classifications.** Some of our data is more confidential than other data. Our Privacy Statement **and the Data Schedule** explains how we classify data and how each type of data should be marked and protected.

6. RETENTION PERIODS

6.1 **Formal or official records.** Any data that is part of any of the categories listed in the Record Retention Schedule contained in the Annex to this policy, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Data Protection Officer.

6.2 **Disposable information.** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

6.3 **Personal data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data. More information can be found in in our Privacy Statement.

6.4 **What to do if data is not listed in the Record Retention Schedule.** If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the Data Protection Officer.

7. STORAGE, BACK-UP AND DISPOSAL OF DATA

7.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

7.2 **Destruction**. Our Data Protection Officer is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be co-ordinated with the Company's IT Provider.

7.3 The destruction of data must stop immediately upon notification from a Director or the Data Protection Officer that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). You will be advised when the actions taken have been resolved and destruction of data can recommence.

8. SPECIAL CIRCUMSTANCES

8.1 **Preservation of documents for contemplated litigation and other special situations.** We require all employees to comply fully with our Record Retention Schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or a Director informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until it has been determined those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact a Director or the DPO.

8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

9. WHERE TO GO FOR ADVICE AND QUESTIONS

9.1 **Questions about the policy.** Any questions about this policy should be referred to a Director or Sam Briggs, the Data Protection Officer, who is in charge of administering, enforcing, and updating this policy.

10. BREACH REPORTING AND AUDIT

10.1 **Reporting policy breaches.** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depend largely on employees. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with a Director. If employees do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

10.2 No one will be subject to and we do not allow, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

10.3 **Audits**. We will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice) to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

11. OTHER RELEVANT POLICIES

11.1 This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:

- IT and communications systems policy.
- Privacy standard.
- Confidentiality policy.
- Use of Social Media Policy

All of which can be found in the staff handbook.

ANNEX A DEFINITIONS

Data: all data that we hold or have control over and therefore to which this policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

Data Protection Officer: our Data Protection Officer who is responsible for advising on and monitoring compliance with data protection laws.

Data Retention Policy: this policy, which explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

Disposable information: disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule.

Formal or official record: certain data is more important to us and is therefore listed in the Record Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

Non-personal data: data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.

Personal data: any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health data and Pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Record Retention Schedule: the schedule attached to this policy which sets out retention periods for our formal or official records.

Storage limitation principle: data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the GDPR as the principle of storage limitation.

ANNEX B RECORD RETENTION SCHEDULE

CLANCY BRIGGS LIMITED (TRADING AS CLANCY BRIGGS CYCLING ACADEMY) establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

Employees should comply with the retention periods listed in the record retention schedule below, in accordance with the policies outlined in this document.

If you hold data not listed below, please refer to a Director or the Company Data Protection Officer. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this record retention schedule, please contact Sam Briggs, Data Protection Officer

TYPE OF DATA	RETENTION PERIOD	REASON / COMMENTS
Recruitment and Payroll records		
Personal information which will include: Application form or CV when applying for the role Home address Date of Birth Emergency contact details Previous employment history Equal opportunities monitoring data such as ethnicity; sexual orientation; religion	Whilst in employment 3 years after employment has ended unless there is an ongoing legislative process in place	Information required for employment record and to advise third parties such as HMRC; payroll provider
Criminal convictions – Disclosure and Barring Check	DBS check will be in the possession of the employee and the employer's record will only be retained to confirm successful completion of check	To ensure that all members of staff meet the safeguarding requirements of the organisation and are able to work with children and young people/vulnerable persons
Employment information: Salary including bank details; tax code, national insurance information Pension information including date of birth, address and next of kin Sickness absence data including	Whilst in employment 3 years after employment has ended unless there is an ongoing legislative process in place	Information required for employment record and to advise third parties such as our HR provider; occupational health provider; payroll provider to make informed decisions during employment To comply with H&S legislation and to advise RIDDOR of

any details of disability or long term condition Information relating to performance including appraisal; disciplinary and grievance issues Accidents and work including nature of accident and any injury sustained Access to email/IT systems including monitoring of inappropriate websites CCTV footage may be kept by specific venues where activities are taking place.		notification of absence relating to injury at work IT provider may be provided with name and job title of employee if concerns raised about access to IT systems which is against Company policy Police or safeguarding lead at Local authority for investigations into concerns regarding safeguarding Concerns regarding timekeeping or fraudulent claims of expenses for example
Termination of employment details which will include: Termination payments including salaries Reference provided to new employer (if requested) Forwarding address	Whilst in employment 3 years after employment has ended unless there is an ongoing legislative process in place	Information required to advise third parties including HMRC; payroll provider (production of P45) production of P60
Suppliers		
Names and addresses of suppliers of goods and services including: Contact details Address and Company information (including registration number) Bank Details (for invoicing purposes)		Information required to order and pay suppliers of goods and services the Academy may use and share with Company accountant. Third party provider details may be passed on our Accountant.

Client information:		
Names and addresses of service users; Contact details for service user representative (if under the age of 18) Photos and videos of activities undertaken	For the period of time the service user is actively using the services of the Academy	Consent from service user to retain information for safeguarding purposes and to arrange for any invoicing of fees for services provider Local Authority if safeguarding concerns are raised during activities
Email address and contact details	For the period of time the service user is actively using the services of the Academy	Where client has shared as part of social media campaigns and have authorised collection of data as part of data processing/information sharing agreement
Name, address, email address and delivery address for on-line customers purchases goods from the website. Name, address and email address of those who have confirmed they wish to receive news of offers on the website.	For the period of time the service user is actively using the services of the Academy	The name and address will be shared with the courier delivering the goods ordered.
Bank or building society details of customers using the website to order goods	For the period of time the service user is actively using the services of the Academy	