THE DOG TRAINING COMPANY
EST. 2008

The Dog Training Company
Data Protection Policy
1/01/2021

Web Privacy Policy

Who We Are
Our website address is : https://thedogtrainingcompany.uk.

Comments
When visitors leave comments on the site we collect the data shown in the comments form, and also the visitor's IP address and browser user agent string to help spam detection. An anonymised string created from your email address (also called a hash) may be provided to the Gravatar service to see if you are using it. The Gravatar service Privacy Policy is available here: https://automattic.com/privacy/. After approval of your comment, your profile picture is visible to the public in the context of your comment.

Media
If you upload images to the website, you should avoid uploading images with embedded location data (EXIF GPS) included. Visitors to the website can download and extract any location data from images on the website

Cookies
If you leave a comment on our site you may opt in to saving your name, email address and website in cookies. These are for your convenience so that you do not have to fill in your details again when you leave another comment. These cookies will last for one year.
If you visit our login page, we will set a temporary cookie to determine if your browser accepts cookies. This cookie contains no personal data and is discarded when you close your browser.
When you log in, we will also set up several cookies to save your login information and your screen display choices. Login cookies last for two days, and screen options cookies last for a year. If you select "Remember Me", your login will persist for two weeks. If you log out of your account, the login cookies will be removed.
If you edit or publish an article, an additional cookie will be saved in your browser. This cookie includes no personal data and simply indicates the post ID of the article you just edited. It expires after 1 day.

Embedded Content From Other Websites
Articles on this site may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if the visitor has visited the other web site.
These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracking your interaction with the embedded content if you have an account and are logged in to that website.

Who We Share Your Data With
If you request a password reset, your IP address will be included in the reset email.

How Long we Retain Your Data
If you leave a comment, the comment and its metadata are retained indefinitely. This is so we can recognise and approve any follow-up comments automatically instead of holding

them in a moderation queue.
For users that register on our website (if any), we also store the personal information they provide in their user profile. All users can see, edit, or delete their personal information at any time (except they cannot change their username). Website administrators can also see and edit that information.

What Rights You Have Over Your Data

If you have an account on this site, or have left comments, you can request to receive an exported file of the personal data we hold about you, including any data you have provided to us. You can also request that we erase any personal data we hold about you. This does not include any data we are obliged to keep for administrative, legal, or security purposes.

Where We Send Your Data

Visitor comments may be checked through an automated spam detection service.

General Data Protection Policy

1. Introduction

This Policy sets out the obligations of The Dog Training Company and its subsidiaries.

whose registered office is at Bungalow 2 Pointer Farm, Great North Road, Leeds. LS25 5LH ("the Company") regarding data protection and the rights of Staff customers and business contacts in respect of their personal data under UK Data Protection Legislation (defined below).

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of personal data relating to them;
"data controller"	means the person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to staff, customers and business contacts used in our business;
"data processor"	means a person or organisation which processes personal data on behalf of a data

	controller;
“Data Protection Legislation”	means all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the “UK GDPR”), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation;
“data subject”	means a living, identified, or identifiable individual about whom the Company holds personal data;
“EEA”	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
“personal data”	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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 data subject;
“personal data breach”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
“processing”	means any operation or set of operations performed on personal data or 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;
“pseudonymisation”	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable

	natural person; and
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3. Data Protection Officer & Scope of Policy

3.1 The Company's Data Protection Officer is Harry Rice, harry@yorkshiredogtraining.co.uk. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies (including those referred to in this Policy), procedures, and/or guidelines.

3.2 All Directors, Managers and Supervisors are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

3.3 Any questions relating to this Policy, the Company's collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the Data Protection Officer.

4. The Data Protection Principles

The Data Protection Legislation sets out the following principles with which any party handling personal data must comply. All personal data must be:

4.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;

4.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

4.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;

4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for

longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject;

4.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. The Rights of Data Subjects

The Data Protection Legislation sets out the following key rights applicable to data subjects:

5.1 The right to be informed;

5.2 the right of access;

5.3 the right to rectification;

5.4 the right to erasure (also known as the 'right to be forgotten');

5.5 the right to restrict processing;

5.6 the right to data portability;

5.7 the right to object; and

5.8 rights with respect to automated decision-making and profiling.

6. Lawful, Fair, and Transparent Data Processing

The Data Protection Legislation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

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

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

7.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

7.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

7.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

8. Specified, Explicit, and Legitimate Purposes

8.1 The Company collects and processes the personal data as follows:

a) personal data collected directly from data subjects**.**

b) personal data obtained from third parties.

8.2 The Company only collects, processes, and holds personal data for the purposes expressly permitted by the Data Protection Legislation.

8.3 Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data.

9. Adequate, Relevant, and Limited Data Processing

9.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8.

9.2 Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

9.3 Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

10. Accuracy of Data and Keeping Data Up-to-Date

10.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 15 below.

10.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. Data Retention

11.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

11.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

12. Secure Processing

12.1 The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

12.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to

ensure their ongoing effectiveness and the continued security of personal data.

12.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

13. Accountability and Record-Keeping

13.1 The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

13.2 The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects.

13.3 All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of the Data Protection Legislation, this Policy, and all other applicable Company policies.

14. Data Subject Access

14.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

14.2 Employees wishing to make a SAR should do so by email to the Company's Data Protection Officer at harry@yorkshiredogtraining.co.uk

14.3 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

14.4 All SARs received shall be handled by the Company's Data Protection Officer

14.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has

already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

15. Rectification of Personal Data

15.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

15.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

16. Erasure of Personal Data

16.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so.

d) the personal data has been processed unlawfully.

e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation

16.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

16.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

17. **Restriction of Personal Data Processing**

17.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

17.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17.3 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. **Objections to Personal Data Processing**

18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing purposes**.**

18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

19. **Direct Marketing**

19.1 The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:

a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from the Company.

19.2 The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and

must be kept separate from other information in order to preserve its clarity.

19.3 If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

20. Data Breach Notification

20.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

20.2 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

20.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

20.4 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

20.5 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned.

b) The categories and approximate number of personal data records concerned.

c) The name and contact details of the Company's data protection officer.

d) The likely consequences of the breach.

e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

21. Implementation of Policy

This Policy shall be deemed effective as of 01/01/2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Craig Rice

Position:	Director
Date:	1 January 2021
Due for Review by:	Annually