THE FORTUNE CENTRE OF RIDING THERAPY

DATA PRIVACY POLICY

VERSION NO.	PREPARED BY	APPROVAL DATE
1	MPL	

UK GDPR: DATA PRIVACY NOTICE FOR WEBSITES

This is the privacy notice of The Fortune Centre of Riding Therapy.

We respect your privacy and are determined to protect your personal data. The purpose of the privacy notice is to inform you as to how we look after your personal data when you visit our website, regardless of where you visit it from. We will also inform you of your privacy rights and how data protection law protects you.

This privacy notice is provided in a layered format, so you can click through to the specific areas set out below.

FREQUENTLY ASKED QUESTIONS

1. **WHO WE ARE AND IMPORTANT INFORMATION**
2. **THE PERSONAL DATA WE COLLECT ABOUT YOU**
3. **HOW WE COLLECT AND USE YOUR PERSONAL DATA**
4. **WHO WE SHARE YOUR PERSONAL DATA WITH**
5. **INTERNATIONAL TRANSFERS**
6. **DATA SECURITY**
7. **DATA RETENTION**
8. **YOUR LEGAL RIGHTS**
9. **CHANGES TO THIS NOTICE AND YOUR DUTY TO INFORM US OF CHANGES**
10. **QUERIES, REQUESTS OR CONCERNS**

1. WHO WE ARE AND IMPORTANT INFORMATION

What is the purpose of this privacy notice?

This privacy notice aims to give you information on how we collect and process your personal data through your use of this website.

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

You must read this privacy notice together with any other privacy notice that 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.

Data Controller(s)

The Fortune Centre for Riding Therapy (FCRT) is the controller and is responsible for your personal data (collectively referred to as "Fortune College," "we," "us" or "our" in this privacy notice). Our Contact details are:

- Address: Avon Tyrrell, Bransgore, Christchurch, Dorset, BH23 8EE
- Email: enquiries@fcrt.ac.uk
- Telephone: 01425 673297

For all data matters contact Matthew Lewer on 01425 673297

Third-party links outside of our control

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 PERSONAL DATA WE COLLECT ABOUT YOU

Personal data or personal information means any information about an individual from which that person can be identified. You can find out more about personal data from the Information Commissioners Office.

The organisation collects and processes the following personal data:

- Employee data as set out in the Privacy Notice for Employees, Workers, and Contractors, for purposes of administering contracts and payroll.
- Job Applicant data, as set out in the Privacy Notice for Job Applicants, for purposes of making recruitment decisions.
- Student, Associate, and other beneficiary data, as set out in the Privacy Notice for Students, Associates and other beneficiaries, for the purposes of measuring and monitoring progress and achievement, support requirements, safeguarding, preparing for transition and auditing.
- Donor, supporter, facilities hirers, supplier data, as set out in the General Privacy Notice, for the purposes of administering contracts and legitimate FCRT interests.

We also collect, use, and share Aggregated Data. Such as statistical or demographic data for any purpose. This can be derived from your personal data, but it is not considered personal data in law as this data does not directly or indirectly reveal your identity. We may aggregate your usage data to calculate the percentage of users accessing a specific website feature. If we combine or connect aggregated data with personal data so it can directly or indirectly identify

you, we treat the combined data as personal data which will be used in accordance with the privacy notice.

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

Where we need to collect your personal data by law, or under the terms of a contract we have with you and you fail to provide the data when requested, we may not be able to perform the contract we have or are trying to enter with you. In this case, we may have to cancel a service you have with us, but we will notify you if this is the case.

3. HOW WE COLLECT AND USE YOUR PERSONAL DATA

We use different methods to collect data from and about you.

FCRT is committed to adhering to the Data Protection Principles which state:

1. Data must be processed lawfully fairly and in a transparent manner
2. Data must be obtained for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Data processed must be adequate, relevant, and limited to what is necessary.
4. Data must be accurate and where necessary kept up to date; every reasonable step must be taken to ensure date that is inaccurate is erased or rectified without delay.
5. Data must not be kept for longer than is necessary for the purposes for which the data are processed.
6. Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Information is kept and processed about individuals for legal purposes (such as payroll), for administrative purposes and for day-to-day people management. FCRT is aware that to process personal data or sensitive personal data, FCRT must rely on the data being:

- Necessary for the performance of a contract, or;
    - 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 such a contract.
- In preparation for a contract, or;
- To comply with our legal obligations, or
    - Processing your personal data where it is necessary for compliance with a legal or regulatory obligation, we are subject to.
- For our legitimate business interests or;
    - The interests of our business in conducting and managing our business to enable us to give you the best service and the most secure experience. We make sure we consider and balance any potential impact on you and your rights before we

process your personal data for our legitimate business 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 by law).

- To perform a task carried out in the public interest or in the exercise of an official authority

If FCRT wishes to hold and process data which does not fall within the conditions listed above, then it will seek to obtain the consent of the individual.

If it is necessary to obtain consent then FCRT will write to the individual to ask for consent, ensuring that the consent is:

- Freely given, specific, informed, and unambiguous
- Separate from other terms
- Clear and in plain language
- As easy to give as to withdraw
- Explicit for sensitive data
- Given in a way that can be evidenced
- Unless consent to processing data is critical to the performance of a contract, the performance of a contract will not be made conditional on the basis that consent is given

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, with the legal bases we rely on to do so.

Please 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 Matthew Lewer, our Data Protection Officer, if you need details about the specific legal grounds that we are relying on to process your personal data, where more than one ground has been set out in the table below.

Purpose/Activity	***Type of Data***	***Lawful Basis for Processing, Including Basis of Legitimate Interest***
News Letter	Name, email, address and telephone number	Legitimate Interest
Donations	Name, email, address and telephone number	Legitimate Interest
Sponsor a Horse	Name, email, address, telephone number and bank details	Legitimate Interest
Contact the College	Name, email, address and telephone number	Legitimate Interest

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. For more information about the cookies we use, please see our Cookie Policy.

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 our Data Protection Officer, Matthew Lewer.

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

4.WHO WE SHARE YOUR PERSONAL DATA WITH

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

- Providers based in specific countries who provide IT and system administration services
- Professional advisers, including lawyers, bankers, auditors, and insurers who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue and Customs, regulators and other authorities based in the United Kingdom who require reporting of processing activities in certain circumstances.
- Specific third parties listen in the table above
- 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 policy.

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 specific purposes and in accordance with our instructions.

5. INTERNATIONAL TRANSFERS

Transferring Personal Data to a Country Outside the EEA

We confirm that whilst we will transfer data to third parties and suppliers within the EEA, we will not transfer your data to a country outside the EEA.

Whenever we transfer your personal data out of the UK, we ensure a similar degree of protection is afforded to it by implementing safeguards:

Please contact us if you would like further information on the specific mechanism used by us when transferring your personal data out of the UK.

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

We will conduct continuous monitoring of our security systems and implement regular training and awareness training to help prevent data breaches.

Organisational Data Protection Methods

FCRT is committed to ensuring the security of your data and to processing it in line with the Data Protection Rules. As such, the organisation will:'

- Ensure all staff are aware of their responsibilities and FCRT's obligations and responsibilities in relation to data protection.
- Ensure all staff and individuals/organisations who handle data on behalf of FCRT are appropriately trained, and receive refreshed training on a regular basis
- Ensure all staff and individuals/organisations who handle data on behalf of FCRT are regularly monitored, assessed, and reviewed.
- Ensure all organisations who handle data on behalf of FCRT are carrying out data processing in line with the Data Protection Rules.
- Regularly review the FCRT's methods of data collection, handling, processing, and storage.

Privacy Impact Statements

Part of the FCRT's ongoing commitment to ensuring maximum protection for personal data means that FCRT will undertake Privacy Impact Assessments where appropriate. Privacy Impact Assessments will help FCRT consider the processing that is being undertaken, the risk to data subjects and the measures that need to be taken to minimise the risks.

Privacy Impact Assessments will be overseen by Sarah Hough and will be reviewed on a 3-yearly cycle, unless it is deemed that a more frequent review is necessary.

Disclosure and Barring Service Checks (DBS)

It is necessary to obtain an Enhanced Check from the Disclosure and Barring Service (which will include a Barred List Check) for all employees and volunteers, including trustees.

FCRT will seek your permission prior to undertaking a DBS check and understands this data is sensitive and thus all information of this nature will be kept strictly confidential. Disclosures and other confidential documents will be kept in a secure location and access will only be available to authorised individuals.

We will not retain the DBS Certificate for longer than necessary. In general, this will be for a maximum of 6 months to allow for the consideration and resolution of any disputes or complaints. In normal circumstances, after 6 months, the disclosure certificate will be destroyed by suitable. Secure means. The top third of the certificate will be retained for 12 months or until CQC inspections have seen them (not retained if offences shown on the top third).

Other than referred to above, no photocopy or other image of the disclosure will be retained but we will keep a record of the details of the most recent check, namely.

- The date of the disclosure
- The name of the individual
- The type of disclosure
- The unique number issued on the certificate
- The decision taken

This will be kept on file for the duration of the individual's employment and for a period thereafter in line with our Retention Policy.

7. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including 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.

For more information and our retention guidelines, please refer to our Data Retention Policy, which is available upon request.

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

In some circumstances we may anonymise your personal data (so that it cannot be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

8. YOUR LEGAL RIGHTS

Unless subject to an exemption under the data protection laws, you have the following rights with respect to your personal data:

- The right to request a copy of your personal data which we hold about you.
- The right to request that we correct any personal data if it is found to be inaccurate or out of date.
- The right to request your personal data is erased where it is no longer necessary to retain such data.
- The right to withdraw your consent to the processing at any time, where consent was the lawful basis for processing your data.
- The right to request that we provide you with your personal data and where possible to transmit that data directly to another data controller (known as the right to data portability), where applicable, i.e. where our processing is based on consent or is necessary for the performance of a contract with you or where we process your data through automated means.
- The right, where there is a dispute in relation to the accuracy or processing of your personal data to request a restriction is placed on further processing.
- The right to object to our processing of personal data, where applicable, i.e. where our processing is based on the legitimate interests (or in performance of a task in the public interest/exercise of official authority; direct marketing or processing for the purposes of scientific/historical research and statistics).

If you wish to exercise any of the rights set out above, please contact Matthew Lewer.

No fee required – with some exceptions

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 admin fee if your request is clearly unfounded, repetitive, or unnecessary. 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 exercise any of the other rights). This is a security measure to ensure your 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 aim to respond to all legitimate requests within one month. Occasionally, it may take longer than a month if your request is particularly complex or if you have made several requests. In this case, we will notify you and keep you updated.

9. CHANGES TO THIS NOTICE AND YOUR DUTY TO INFORM US OF CHANGES

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

10. QUERIES, REQUESTS OR CONCERNS

To exercise all relevant rights, queries, or complaints in relation to this policy or any other data protection between you and us, please in the first instance contact our Data Protection Officer, Matthew Lewer.

If this does not resolve your complaint to your satisfaction, you have the right to lodge a complaint with the Information Commissioners office on 03031231113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England, UK.