



THE FORTUNE CENTRE OF RIDING THERAPY

DATA PROTECTION POLICY

VERSION NO.	PREPARED BY	TRUSTEE APPROVAL DATE
1	SJH	

Introduction

The Fortune Centre of Riding Therapy (FCRT) is committed to working in accordance with the General Data Protection Regulation (GDPR) and with the highest standards of ethical conduct.

This policy outlines the rules, behaviours and standards required of the organisation, employees, workers and third parties working on behalf of FCRT in relation to the collection, retention, transfer, disclosure, use and destruction of any personal data. All workers will be responsible for data protection and must abide by the rules and policies of FCRT.

Personal Data and Sensitive Personal Data

There are two types of personal data that fall under the GDPR and for which FCRT, its employees, workers and third parties are responsible. These are: -

- Personal Data

This is defined as any information relating to an identified or identifiable natural person. Identification can be by means of "an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." This will include IP addresses and cookie strings.

- Sensitive Personal Data

Sensitive personal data includes data relating to genetic and biometric data as well as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or a person's sex life, sexual orientation or criminal offences.

Data Protection Principles

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 specified, 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 data that are inaccurate, are 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 for payroll), for administration purposes and for the purposes of day-to-day people-management. FCRT is aware that in order to process personal data, or sensitive personal data, FCRT must rely on the data being:

- necessary for the performance of a contract, or;
- in preparation for a contract, or;
- to comply with our legal obligations, or;
- for our legitimate business interests or;
- 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 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.

Personal Data

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.

Rights of Data Subjects

FCRT will recognise that individuals have the following rights under data protection legislation:

- a. the right to be informed, which encompasses the obligation on employers to provide transparency as to how personal data will be used;
- b. the right of access;
- c. the right to rectification of data that is inaccurate or incomplete;
- d. the right to be forgotten under certain circumstances;
- e. the right to block or suppress processing of personal data; and
- f. the new right to data portability which allows employees to obtain and reuse their personal data for their own purposes across different services under certain circumstances.

Right of Access

Individuals have the right to access the information stored about them. Employees can ask for access to their own personal details held electronically or held manually. Employees who wish to see their records should give notice electronically, in writing, using the Subject Access Request Form which can be found on SharePoint. FCRT has up to 1 month to provide the information following the subject access request, which it will usually do in electronic format.

In complex cases, or where there are numerous related requests, FCRT will liaise with the individual to inform them of progress of their request(s), and if it is not possible to complete this within 1 month, FCRT will inform the individual of the delay, the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months.

In the event that data is retained with third parties, FCRT will ensure that the request is communicated and actioned by the third party in line with the timescales outlined above, unless impossible or if it would require disproportionate effort.

FCRT reserves the right to charge a fee or to refuse to respond to a request if it is manifestly unfounded or excessive. Similarly, FCRT reserves the right to withhold personal data if disclosing it would adversely affect the rights and freedoms of others.

Rectification of Data

FCRT is committed to keeping data that is accurate and up to date. Data will be checked for accuracy where possible, and any data that is inaccurate, out of date or unnecessary will be corrected or erased as appropriate.

Where an individual identifies that their personal data is incorrect or incomplete, or where they are aware that their personal data has changed, they must inform the organisation as soon as possible. The organisation will then take steps to rectify any inaccuracies as soon as possible, and at the latest within 1 month.

In complex cases, or where there are numerous cases, FCRT will liaise with the individual to inform them of progress of their request, and if it is not possible to complete this within 1 month, FCRT will inform the individual of the delay and the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months.

In the event that data has been disclosed to third parties, FCRT will ensure that the request for rectification is communicated and actioned by the third party in line with the timescales outlined above, unless this is impossible or if it would involve disproportionate effort.

The Right to be Forgotten

Also known as 'the right to erasure', the right to be forgotten doesn't provide an absolute right to be forgotten, but data subjects have a right to have personal data erased and to prevent processing in some circumstances i.e.

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data has to be erased in order to comply with a legal obligation;
- The personal data is processed in relation to the offer of information society services to a child.

If you wish to ask for your own personal data to be partially/fully erased and no longer processed, please write to Sarah Hough with full details of your request. FCRT has up to 1 month to respond to you and either delete the data or explain why it is unable to comply with your request. Circumstances where FCRT may be unable to comply include where it is required to retain the information by law, or if the data is needed in connection with legal proceedings.

In complex cases, or where there are numerous related requests, FCRT will liaise with you to inform you of progress of the request, and if it is not possible to respond to this within 1 month, FCRT will inform you of the delay, the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months, if necessary.

In the event that data is retained with third parties, FCRT will ensure that the request is communicated and if appropriate actioned by the third party in line with the timescales outlined above.

Security of Data

FCRT is committed to taking steps to ensure that personal data is protected, and to prevent any unauthorised access, accidental loss, destruction, unlawful processing, equipment failure or human error, and will do this through the continual monitoring of our security systems and by regular training and awareness raising.

Any data breaches or near misses, will be managed according to the procedures documented in our Data Protection Breach Reporting Policy and Procedure.

Data Retention

FCRT is committed to ensuring that subject data is kept for no longer than necessary and only kept as long as it's relevant and necessary for legitimate purposes. As soon as data is no longer necessary for the purposes for which it was originally collected, it will be securely deleted, unless it is necessary to keep the data for some other legitimate reason.

FCRT does not intentionally keep data longer than necessary and when data is no longer required, FCRT is committed to securely deleting it as soon as possible.

For more information and our retention guidelines, please refer to our Data Retention Policy.

Data Breaches

All staff are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach has been discovered, where possible, the member of staff should complete a Data Protection Breach Reporting Form (to the fullest extent possible at that time), which provides full details concerning the breach. This form should then be passed to Sarah Hough, Head of Finance as soon as possible on the discovery of the breach. If you need help completing the form, or are unable to complete the form, then any delay should be avoided and instead the matter should be reported immediately, either verbally or using electronic means, such as email.

For more information regarding managing data protection breaches, please refer to the Data Protection Breach Reporting Policy and Procedure.

Transferring Personal Data to a Country Outside the EEA

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

Data Portability

On occasion you may wish to allow your data to be transferred to another Organisation either by you receiving the data and transferring it, or by the data being transferred directly.

This right to data portability only applies to data that you have provided to FCRT, where the data processing is based either on your consent or the performance of the contract and where the processing is carried out by automated means, and it will only be transferred where it is technically feasible to do so.

If you wish to make a request for your data to be transferred, you must write to Sarah Hough, and we will respond to you within 1 month. If the requests are numerous or complex we reserve the right to extend this timescale by a further 2 months. If we are unable to complete your request, we will write to you to inform you why, along with your right to complain to the Information Commissioner's Office (ICO).

Objections to Personal Data Processing

You have the right to object to data processing where FCRT is:

- processing information based on its legitimate business interests, or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing
- processing for the purposes of scientific/historical research and statistics.

If you wish to object to processing, you should write to Sarah Hough outlining the grounds relating to your particular situation and we will stop the processing unless we have compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is in relation to legal claims. If we are unable to agree to your request, we will write to inform you why, along with your right to complain to the ICO.

Organisational Data Protection Measures

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 that all staff are aware of their responsibilities and FCRT's obligations and responsibilities in relation to data protection;
- Ensure that all staff and individuals/Organisations who handle data on behalf of FCRT are appropriately trained, and receive refresher training on a regular basis;
- Ensure that all staff and individuals/Organisations who handle data on our behalf are regularly monitored, assessed and reviewed;
- Ensure that all Organisations who handle data on our behalf 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 Assessments

As part of FCRT's ongoing commitment to ensuring maximum protection for personal data, 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 most importantly 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 that this data is sensitive data and therefore 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 a period of 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 inspectors have seen them (not retained if offences shown on the top third). Other than as 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 and 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.

Data Protection Officer

FCRT has appointed a Data Protection Officer, who will support the organisation to manage Data Protection and will work with the Trustee Board in this respect. Any queries or concerns can be addressed directly to the Data Protection Officer – Sarah Hough at Avon Tyrrell.

Monitoring

We are committed to monitoring this policy and will update it as appropriate, on an annual basis or more frequently if necessary.

Any queries or concerns can be addressed directly to Sarah Hough