PRIVACY NOTICE – SERVICE USERS

Reviewed August 2025

1. Introduction

CF Education and CF Social work, known as CF Group, treats the privacy of our service users' personal data seriously. This notice identifies for you some key information about data processing and sets out the type of data we collect from you, why we collect it and how we manage it. Managing data includes identifying the lawful basis for processing data, as well as how we gather, store, process, share, protect and ultimately destroy data.

Our responsibilities relating to data processing are set out in the General Data Protection Regulations (GDPR) and Data Protection Act (2018). In line with these provisions, data processing is overseen by our designated Data Protection Officer (DPO) whose principal duties are to inform, advise and monitor CF Group's compliance with the GDPR.

Our policies in relation to Data Protection are set out in the following policies:

- GDPR Policy and Procedure
- Data Protection and Confidentiality Policy and Procedure
- Data Security and Data Retention Policy and Procedure
- Service User Privacy Policy and Procedure
- Subject Access Requests Policy and Procedure

If you wish to receive copies all of the above policies please request these in writing.

2. What is Personal and Sensitive Data?

Personal data means any information that may be used to identify you on its own or when combined with other information, will enable identification. **Sensitive data** is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation. We may collect, use, store and transfer different kinds of personal and sensitive data about you which we have grouped together as follows:

a) **Identity Data** includes first name, last name, username or similar identifier, date of birth and gender and NHS number.
b) **Contact Data** includes your address, phone number and email address.
c) **Health Data** includes any information about your physical or mental health from how you use our Services.
d) **Usage Data** includes information about how you use our services.

3. Why do we collect your data?

Your personal data is required to effectively provide you with our services. In addition, key data may be used to support our safeguarding responsibilities and other statutory obligations. We also require your data to measure the effectiveness of the services we provide and how they can be improved. This uses aggregated statistics which does not identify you.

4. How do we obtain your data?

We use different methods to collect data from and about you including through:

a. **Direct interactions:** You may give us any of the categories of data identified in section 2 by filling in forms or by corresponding with us by, phone, email or otherwise.

b. **Third Parties:** We may receive your personal data from third parties who are referring you to our services. This is typically performed with your explicit consent but could be because there is a legal obligation that applies to the third party.

5. What do we do with your data?

All of the data gathered is processed to effectively assess you for our services and provide you with a service accordingly. Our lawful reasons for processing data are detailed in the table below along with the type of data. 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.

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
To register you as a new service user	(a) Identity (b) Contact	Necessary for our legitimate interest to provide our services to you
To process and deliver a request for our services.	(a) Identity (b) Contact (c) Health	Necessary for our legitimate interests (to provide our services to you) Article 9 of the GDPR and Schedules of the Data Protection Act 2018
To manage our relationship with you	(a) Identity (b) Contact	Necessary to comply with a legal obligation Necessary for our legitimate interests (to keep our records updated and to study how service users use our services)
To comply with Information Sharing Agreements which can be for the purpose of Adult and Children Safeguarding.	(a) Identity (b) Contact (c) Usage	Necessary in order to protect the vital interests

To administer and protect our business and online services (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	a. Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) b. Necessary to comply with a legal obligation
To use data analytics to improve our services, relationships and experiences	((b) Usage	Necessary for our legitimate interests (to define types of service users for our services, to keep our services updated and relevant, to develop our business)

We will not use the personal data for marketing purposes. We will only use your contact details to correspond with you about the services we provide you with.

As part of our safer recruitment procedures and to comply with Ofsted requirements, a copy of your DBS is securely stored in a separate location from everyday recruitment and HR files, with access restricted to the recruitment team

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 us. 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.

6. Record Keeping

We keep files on all our service users but only keep relevant information to ensure that the service we offer as an organisation is of the highest quality. The files are only available to staff who need to use them.

We make sure that:

- records required for the protection of service users and for the effective and efficient running of the service are maintained, are up to date and are accurate
- service users have access to records and information about them held by the service, as well as opportunities to help maintain their personal records
- individual records and care service records are kept in a secure fashion, are up to date and in good order, and are constructed, maintained and used in line with the General Data Protection Regulation and the Data Protection Act 2018 and other statutory requirements. CF Group adheres fully to the current standards on record keeping as set by the ICO

- CF Group considers that access to information and security and privacy of data is an absolute right of every service user and that service users are entitled to see a copy of all personal information held about them and to correct any error or omission in it.

7. Data Storage

We take the security of personal data seriously. Your personal data is stored in electronic and paper files. The organisation has internal policies and controls in place to try to ensure that data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. This includes:-

- An Internet facing firewall to prevent outside penetration of the organisations network. Policies allow mail to be delivered into the mail server from a specific set of addresses (our external spam filter) but no other access is allowed. This firewall also maintains a list that prevents access to malicious sites on the WWW.
- Cyber Essentials is installed across the company
- Spam filtering. All our mail passes through a spam filter which looks for unsolicited mail, malicious software and dangerous links.
- Local firewalling. All our machines are individually protected by firewalls. This prevents problem software proliferating through the network and unauthorised access from one machine to another e.g. only the IT department can remotely connect to a Company laptop.
- Local anti-virus to prevent any malicious software getting through the firewall or spam filters or be brought in by other means. Every machine in the Company has anti-virus software installed which is constantly updated via a server on the network. This software also maintains a web blacklist to prevent access to malicious sites.
- File access controls. Access to data on the servers is controlled based on need. Management authority is required before any changes of access are made.
- Encryption. All Company emails are encrypted when the recipient supports encryption.
- Filing cabinets. Data kept in service users' files are stored in lockable cabinets and secured in a restricted office however paper copies are kept to a minimum
- IT Policy. This policy is to ensure that all information

technology users within the organisation or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organisations boundaries of authority.

- Social Media Policy. This policy is aimed to educate employees and minimise risks when using social media which can impact the organisation and employees.

8. Sharing your Data

Data is shared within the organisation as part of our lawful basis to process and is only shared relevant to the processing requirement. We will not share data with third parties unless there is a lawful / regulatory / legal / contractual requirement or where you have given clear consent. We will aspire to share the minimum amount of data necessary for the purpose and restrict the use of data that directly or indirectly reveals your identify. This can include anonymising your data or producing aggregated statistics or demographic information.

Examples of where we share such information in line with the above include:

a. Safeguarding obligations
b. Ofsted obligations
c. Contractual reporting
d. Health and Social Care Datasets
e. A referral made on your behalf with your clear consent
f. A referral made for medical purposes including to protect your vital interests.
g. With any purchaser of the business in order to allow transfer of data to the buyer

We do not transfer any of your personal data outside of the European Economic Area.

Examples of third parties include but are not restricted to Local Authorities, Clinical Commissioning Groups (CCGs), Public Health England (PHE), NHS Digital, Housing Associations, Hospital units, etc.

9. Retaining your data

We retain service users information only for as long as is necessary to provide the service. We will usually delete all your personal data within 12 months of our service to you ending. This is set out in CF Group's Data Security and Data Retention Policy and Procedure

10. Privacy Notice - Data Subject Rights

The following information is intended to help you understand you rights in relation to personal and sensitive data as provided by either the Data Protection Act (2018) or the General Data Protection Regulation 2016.

The right to be informed: This relates to what information we are required to provide you with about data processing. This Privacy Notice represents the way in which we inform you of this information.

Right of access: You (i.e. the data subject) have the right to access particular personal and sensitive information that we hold about you. This is known as a Subject Access Request. We shall respond promptly (usually within one month from the point of receiving the request and all necessary information from you). This provision is usually free of charge.

Right to rectification: You have the right to obtain from us, without undue delay, the rectification of inaccurate or incomplete personal data that we hold concerning you.

Right to erasure: You have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. We have the right to refuse to comply with a request for erasure and if this applies, we will tell you the reason why.

Right to restrict processing: Subject to exemptions, you shall have the right to restrict processing where:

- You contest the accuracy of the information we hold and it is restricted until the accuracy is verified,
- You have objected to processing (where it is necessary for the performance of a public interest task / legitimate interest) and we are considering whether our grounds override your rights
- Processing is unlawful and you oppose erasure, requesting restriction instead,
- We no longer need the data, but you require the data to establish, exercise or defend a legal claim.

Right to Data Portability: This applies when processing is carried out in an automated way. You shall have the right to receive the personal data you have provided to us in a structured, commonly used and machine-readable format. Where technically feasible, this right extends to us transmitting the data to another organisation at your request. For data portability to apply, the processing of your data must relate to information that is either i) based on your consent or ii) processed for the performance of a contract.

Right to Object: You have the right to object to processing on grounds relating to your personal circumstances. This provision applies to the processing that is undertaken for legitimate interests / the performance of a task in the public interests (includes personal profiling) and processing for purposes of scientific / historical research and statistics. In such cases we will stop processing unless we can demonstrate i) compelling legitimate grounds which override your interests, rights and freedoms ii) the processing is for the establishment

, exercise or defence of legal claims. This right extends to processing for the purposes of direct marketing (including profiling) which must be stopped outright.

Right to Complain to the Information Commissioners Office: You have the right to complain to the Information Commissioners Office at any time.

Right not to be subject to decisions based solely on automated processing: We do not carry out any automated processing which may lead to automated decision making based on your personal data.

Information accuracy: We take all reasonable steps to ensure the accuracy of the personal/ sensitive data that we hold and provide

Invoking your rights: If you would like to invoke any of these rights, please write to:

The Data Protection Officer
CF GroupLtd
3-4b K Line House, West Road, Ipswich, SUFFOLK, IP3 9SX
01473 725 794
Email: nina@cfsocialwork.co.uk