Data Protection Policy

INTRODUCTION

The Data Protection Act 2018 (DPA) sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It sits alongside the UK General Data Protection Regulation (UK GDPR) which sets out the key principles, rights and obligations for most processing of personal data. The DPA tailors how the UK GDPR applies - for example by providing exemptions. The Regulations, which apply to both client and employee data, cover both written and computerised information and the individual's right to see such records.

The following guidance is not a definitive statement on the Regulations but seeks to interpret relevant points where they affect HEADS UP REHABILITATION LIMITED.

All employees, associates and agents of HEADS UP REHABILITATION LIMITED must adhere to this Policy at all times. Any deliberate or reckless breach of this Data Protection Policy by any employee or contractor of HEADS UP REHABILITATION LIMITED may result in disciplinary action and/or dismissal.

CONTENTS

Data Protection Policy

DEFINITIONS

Data Subject	An individual about whom data is processed.
Data Controller	The individuals responsible for the entity with overall responsibility for data processing. For the purposes of the DPA, the Directors of HEADS UP REHABILITATION LIMITED are the Data Controllers.
Data Processor	Any third-party individual or organisation processing data on behalf of / at the instruction of the Data Controller. (Note that this does not include employees - employees processing personal data within the organisation do so to fulfil our tasks as data controller.)
Personal Data	Any information that relates to an identified or identifiable individual person. Note this applies whether the data is factually accurate or not. See here for more details about what constitutes personal data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/key-definitions/what-is-personal-data/
Data Processing	Any use of Personal Data, including collecting, storing, transferring, in both electronic and hard copy format.
Special Category Data	Information which is particularly sensitive, and thus requires further protections.

DATA PROTECTION PRINCIPLES

As a Data Controller we are obliged to comply with the following principles:

1. Process personal data fairly, lawfully and in a transparent manner.
2. Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held.
4. Ensure that personal data is accurate and, where necessary, kept up-to-date.
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the United Kingdom unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

DATA SUBJECTS RIGHTS

All data subjects have a number of rights that we must always act on when they request to exercise these rights by contacting us. They have the right to:

- Be informed about how, why and in what ways we will process their personal data.
- Request to see or have a copy of all data we are holding that relates to them (known as a “data subject access request”);
- Request us to amend incorrect or incomplete data;
- Request us to erase their personal data;

- Request us to stop processing their data in certain ways (right to "restricted processing");
- Request that we pass their personal data onto another organisation (right to "data portability"). *This right only applies to personal data that is processed under the consent or contract basis, is processed by automated means and is data that has been provided to you by the data subject. In the event of an appropriate request, we will transfer the data in an electronic format to either the data subject or the organisation they have requested*;
- Object to the processing of the data. *This right only applies to personal data that is: processed under the legitimate interests basis; used for public interest tasks; used to exercise an official authority, or; used for direct marketing purposes.*

HEADS UP REHABILITATION LIMITED does not carry out any electronic profiling or automated decision making.

Data subjects also have a right to make a complaint to the Information Commissioner's Office if they feel we are not meeting our obligations under the UK GDPR or DPA.

INFORMING INDIVIDUALS OF DATA PROCESSING

HEADS UP REHABILITATION LIMITED may collect and process personal data for the following individuals:

- Clients and their family members
- Contracted service providers (e.g. self-employed occupational therapists)

Each individual, upon engaging with HEADS UP REHABILITATION LIMITED, will be provided with a relevant Privacy Statement or Private Notice informing them of the following:

- Who the Data Controller is and their contact details.
- What lawful basis is being utilised to process their personal data.
- What personal data will be collected and processed.
- Why the data is being collected and processed.
- How long their personal data will be retained for.
- How they can enact their rights under the UK GDPR, which will vary depending on what lawful basis their personal data is collected under.

LAWFUL BASES FOR DATA PROCESSING

Under the UK GDPR, there are six lawful bases for processing personal data. Most lawful bases require that processing is 'necessary' for a specific purpose; If the same purpose can be reasonably achieved without the processing, then no lawful basis will apply.

The six lawful bases are:

a. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
b. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d. Vital interests: the processing is necessary to protect someone's life.
e. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

It is generally expected that HEADS UP REHABILITATION LIMITED, in the course of its regular business activities which require processing of personal data, will process under the bases of a. Contract, b. Legal Obligation and c. Consent. In the event of an emergency, data may also be processed under d. Vital Interests. Where it is necessary for personal data to be processed under another lawful basis, this will be documented in advance of processing the data, including the reasons why the processing is necessary.

SPECIAL CATEGORY DATA

It is expected that in the execution of its services, HEADS UP REHABILITATION LIMITED will need to process sensitive personal data. Data that is classified as sensitive is information that could create more significant risks to a person's fundamental rights and freedoms, for example, by putting them at risk of unlawful discrimination. Examples of sensitive data include information about an individual's:

- race or ethnic origin;
- religion;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sexual orientation;
- criminal convictions.

All special category data being processed must meet specific conditions under UK GDPR or be allowable through the DPA, in addition to meeting one of the six lawful bases for its processing. These conditions can be found in Article 9(2) of the UK GDPR, and are listed in detail here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/lawful-basis-for-processing/special-category-data/.
In summary the conditions are:

a. The data subject has given explicit consent to the processing for a specified purpose(s).
b. Processing is necessary for the controller to carry out their obligations as an employer.
c. Processing is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.
d. Processing is carried out in the course of its legitimate not-for-profit activities with a political, philosophical, religious or trade union aim.
e. Processing relates to personal data which are manifestly made public by the data subject.
f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g. Processing is necessary for reasons of substantial public interest, on the basis of law.
h. Processing is necessary for the purposes of preventive or occupational medicine, assessment of working capacity of an employee, medical diagnosis or provision of healthcare treatment.
i. Processing is necessary for reasons of public interest in the area of public health or to ensure high standards of quality and safety of health care.
j. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

It is generally expected that HEADS UP REHABILITATION LIMITED, in the course of its regular business activities which require processing of sensitive personal data, will be doing so in order to meet conditions; a. Consent; b. Employer obligations (this includes requesting DBS checks for Directors*); c. Protecting vital interests of individuals without capacity; or h. For provision of healthcare treatment. Where it is necessary for sensitive personal data to be processed under a different condition, this will be documented in advance of processing the data, including the reasons why the processing is necessary.

*Special note with regards to criminal records data – DBS checks are lawfully able to be carried out on staff/contractors because they are to be working with children or vulnerable adults (as per Schedule 1 of the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975), however in general, the resultant criminal records data from such checks should only be retained in exceptional circumstances. Otherwise it is appropriate to simply retain the record of the DBS certificate number, the date it was issued and whether the check was clear or not.

DATA SUBJECT ACCESS REQUESTS

Whenever a data subject access request is made, we will follow these steps:

1. Ensure there is a written record of the request including the date and method the request was made (e.g. verbally, posted letter, email).
2. Respond to the individual within 72 hours receipt of their request to acknowledge the request and inform them that we will begin the task of reviewing it and that we have 1 month to respond/enact this.
3. Research the full details of our obligations under the UK GDPR and which apply to the specific situation. More details can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/individual-rights/right-of-access/
4. When enacting the request is expected to take longer than 1 month, we will inform the data subject before the original deadline and can extend the deadline by up to 2 months, if it is reasonable to do so (e.g. there are multiple requests or the request is very complex).
5. If we believe it is within reason to refuse the request, we will document our justification for this decision and inform the data subject prior to the 1 month deadline. We must tell them why we are refusing the request, that they have the right to complain to the ICO and that they can seek a judicial enforcement to the request if they wish to.

6. If we agree to the request, we will provide the data to them. Where possible this should be digitally, via a secure self-service system (e.g. a shared Dropbox folder or link to a secure file-sharing platform).

DATA RECTIFICATION REQUESTS

Whenever a data subject requests we amend data that is inaccurate (incorrect or misleading) or missing, we will follow these steps:

1. Ensure there is a written record of the request including the date and method the request was made (e.g. verbally, posted letter, email).
2. Respond to the individual within 72 hours receipt of their request to acknowledge the request and inform them that we will begin the task of reviewing it and that we have 1 month to respond/enact this.
3. We will restrict further processing of the data in question whilst its accuracy is examined.
4. Research the full details of our obligations under the UK GDPR and which apply to the specific situation. More details can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/individual-rights/right-to-rectification/
5. When enacting the request is expected to take longer than 1 month, we will inform the data subject before the original deadline and can extend the deadline by up to 2 months, if it is reasonable to do so (e.g. there are multiple requests, the request is very complex or we need more time to consider the accuracy of the disputed data).
6. If we believe it is within reason to refuse the request, we will document our justification for this decision and inform the data subject prior to the 1 month deadline. We must tell them why we are refusing the request, that they have the right to complain to the ICO and that they can seek a judicial enforcement to the request if they wish to.
7. If we agree to the request, we will correct the data and write to the data subject to inform them that the data has been rectified. We must also contact any recipients with whom the data has been shared and inform them of the rectification. Where this is the case, we must also inform the data subject about these additional recipients.

RESTRICTED PROCESSING

Whenever a data subject has made a request for erasure or amendment of their personal data or objected to its processing, we must restrict use of their data until the situation is resolved. This means we can store the data but must not use it in any other way unless we have the data subject's consent, the use is for exercise or defence of a legal claim, the use is to protect another person, or it is for reasons of important public interest. We will add a note to our electronic and any paper filing systems to state that processing of the individual's data is restricted and, where possible, put electronic means in place to prevent any further amendments to or use of the data.
It is also possible for data subjects to request restriction of the processing of their data. More details about this can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/individual-rights/right-to-restrict-processing/

Data Protection Policy

ENSURING THE SECURITY OF PERSONAL DATA

Staff must at all times avoid unlawful disclosure of personal information and therefore should be aware of the following:

- It is an offence to disclose personal information 'knowingly and recklessly' to third parties.
- Client's consent to share information should always be checked before disclosing personal information to another organisation or individual.
- Where client's have given their consent for us to share their personal or special categories of personal data with others, this should only be shared on a "need-to-know" basis.
- Where such consent does not exist, information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case, permission from one of the Company Directors should first be sought.
- Care should be taken that conversations containing personal or special categories of data may not be overheard by people who should not have access to such information.

In order to prevent unauthorised access or accidental loss or damage to personal data, it is important that care is taken to protect such data. Paper records should be kept in locked cabinets/drawers when not in use and care should be taken that personal and special category data is not left unattended or in clear view whilst in use. If your work involves you having personal and sensitive data at home or in your car, the same care needs to be taken. When transporting documents, they should be carried out of sight in the boot of your car. Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. All paper containing personal/sensitive data, once no longer required, should be securely shredded.

When working with personal or sensitive data on a computer, the screen/monitor should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. If working in a public area the computer must be "locked" if leaving it unattended. Firewalls and virus protection must be in place at all times on any computers used for work purposes to reduce the possibility of hacking or data corruption. Documents containing personal data should be stored on a secure cloud-based system and not kept longer than necessary on individual computer hard drives. All computers and devices used to access cloud-based services containing personal data must be password protected.

RETENTION AND ERASURE OF PERSONAL DATA

HEADS UP REHABILITATION LIMITED will only hold personal data for as long as is necessary to fulfil the purposes we collected it for. For self-employed service providers, this will be 7 years after termination of contract. For clients, this will be 7 years after they cease using our services except where the client is a child, in which case it will be until their 25th birthday. Where we believe there is a chance of future litigation, we may retain a client's data for

longer than this. Where this is the case it will be documented in their records as to why the data is being retained and for how long this is expected.

When a data subject requests for their personal data to be erased from our records, we will follow these steps:

1. Ensure there is a written record of the request including the date and method the request was made (e.g. verbally, posted letter, email).
2. Respond to the individual within 72 hours receipt of their request to acknowledge the request and inform them that we will begin the task of reviewing it and that we have 1 month to respond/enact this.
3. Ensure the right to erasure applies. This will be the case if:
    a. the personal data is no longer necessary for the purpose which we originally collected or processed it for;
    b. we are relying on consent as our lawful basis for holding the data, and the data subject has withdrawn their consent;
    c. we are relying on legitimate interests as our basis for processing, the data subject has objected to the processing of their data, and there is no overriding legitimate interest to continue this processing;
    d. we are processing the personal data for direct marketing purposes and the data subject objects to that processing;
    e. we have processed the personal data unlawfully;
    f. we have to erase the data to comply with a legal obligation; or
    g. we have processed the personal data to offer information society services to a child.

    The right to erasure will not apply if our processing of it is necessary for one of the following reasons:
    a. to exercise the right of freedom of expression and information;
    b. to comply with a legal obligation;
    c. for the performance of a task carried out in the public interest or in the exercise of official authority;
    d. for archiving purposes in the public interest (scientific research, historical research or statistical purposes); or
    e. for the establishment, exercise or defence of legal claims.

    Additionally, if the request relates to special category (sensitive) data, the right to erasure will not apply if:
    a. the processing is necessary for public health purposes in the public interest (e.g. ensuring high standards of quality and safety of health care); or
    b. the processing is necessary for the purposes of preventative or occupational medicine (e.g. for establishing the working capacity of an employee; for medical diagnosis; for the provision of health or social care).
4. Research the full details of our obligations under the UK GDPR and which apply to the specific situation. More details can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-GDPR/individual-rights/right-to-erasure/
5. When enacting the request is expected to take longer than 1 month, we will inform the data subject before the original deadline and can extend the deadline by up to 2 months, if it is reasonable to do so (e.g. there are multiple requests or the request is very complex).

6. If we believe it is within reason to refuse the request, we will document our justification for this decision and inform the data subject prior to the 1 month deadline. We must tell them why we are refusing the request, that they have the right to complain to the ICO and that they can seek a judicial enforcement to the request if they wish to.
7. If we agree to the request, we will erase the data, including from any backup systems, and write to the data subject to inform them that the data has been erased. We must also contact any recipients with whom the data has been shared and inform them of the erasure. Where this is the case, we must also inform the data subject about these additional recipients.

COMPANY ACCESS AND SHARING OF PERSONAL DATA

All personal data stored by HEADS UP REHABILITATION LIMITED will be accessible by the Directors. Access to other staff members will be restricted and access will only be provided on a "need-to-know" basis. Where possible, staff will be given direct, but limited, access to data storage systems or where this is not possible, data will be shared using a secure transfer method.

Personal data will only be shared with third parties where required by law, where it is necessary in order to administer our working relationship, or where we have the data subjects' explicit consent to do so. In all circumstances where data is shared with third parties, the data will be subject to confidentiality arrangements.

It is not expected that HEADS UP REHABILITATION LIMITED will ever need to transfer personal data to individuals outside the United Kingdom, but should this need ever arise, we will seek the data subjects' explicit consent to do this. The exception to this is in regards to online software service providers who may have servers outside the United Kingdom. In these instances, HEADS UP REHABILITATION LIMITED will ensure that these online services have adequate Standard Contractual Clauses in place before inputting any client/associate personal data.

COLLECTING PERSONAL DATA VIA ONLINE FORMS

Personal data may be collected about individuals via online forms, for example digital questionnaires or via the contact form on our website.

Any digital forms that contain personal data should be password protected and the access links only shared with relevant persons who need to access them.

Any publicly accessible online forms that request the input of personal data should include the following statement:

We promise never to share or sell your information to other organisations or businesses, unless we have your explicit consent to do so, and you can opt out of our communications at any time by emailing gaynor@headsuphealth.co.uk.

Data Protection Policy

DIRECT MARKETING

Direct Marketing is a communication that seeks to inform recipients of our services and to elicit a response, such as engaging in our services. The communication may be in a variety of formats including mail, telephone marketing and email.

HEADS UP REHABILITATION LIMITED does not currently maintain a mailing list and it is not expected that unsolicited marketing communication should be carried out at any time.

WHAT TO DO IN THE EVENT OF A DATA BREACH

A 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. Data breaches could include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

If any staff member discovers, or suspects, a data breach, this should be reported immediately. One of the Directors or a nominated Data Protection Champion will then:

1. Record details of the perceived breach, including date, time, who reported it and the nature of the breach.
2. Conduct an immediate review of our systems, in order to prevent a continuation of the breach or a reoccurrence.
3. Conduct a review of the breach to determine if the ICO need to be informed. This must be completed and the ICO informed (if necessary) within 72 hours of the breach occurring. The ICO should be informed if it is felt there is a risk to the rights and freedoms of the data subjects to whom the data relates or if the breach relates to a large volume of personal data. If the breach does need to be reported, we will inform the ICO of:
    a. The number of data subjects involved;
    b. The type and amount of data involved;
    c. The likely consequences of the breach;
    d. The measures taken to deal with the breach and to mitigate any potential adverse effects;
    e. The name of the relevant company contact for the ICO to respond to.
4. Regardless of if the breach is reported to the ICO or not, record details of the breach, any actions taken, and the reasoning for all decisions made.