DATA PROTECTION POLICY

Introduction

Vital 24 Healthcare Ltd is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, people it supports and all Stakeholders under applicable Data Protection Law.

POLICY STATEMENT

Vital 24 Healthcare Ltd is committed to complying with data protection law as part of everyday working practices. Complying with data protection law may be summarised as but is not limited to:

Understanding, and applying as necessary, the data protection principles when processing personal data.

Understanding, and fulfilling as necessary, the rights given to data subjects under data protection law and understanding and implementing as necessary Vital 24 Healthcare Ltd's accountability obligations under data protection law.

PURPOSE AND SCOPE

The purpose of this policy is to ensure compliance with the General Data Protection Regulation (GDPR) and related EU and national legislation (Data Protection Law).

Data Protection Law applies to the handling and storing ("processing") of information ("personal data") about identifiable individuals ("data subjects").

This policy sets out how Vital 24 Healthcare Ltd deals with personal data, including personnel files and data subject access requests, and rights and obligations in relation to personal data.

This policy applies to all business areas within Vital 24 Healthcare Ltd ("data controller" and "data processors").

This policy is not and should not be confused with a privacy notice (a statement informing data subjects how their personal data is used by Vital 24 Healthcare Ltd).

This policy should be read in conjunction with the obligations in the following documents which supplement this policy:

-Confidentiality Policy

-Applicable Privacy Notices – workers and clients

-Management Reference Guides

-Staff employment contracts and comparable documents (e.g. workers handbook) which impose confidentiality obligations in respect of information held by Vital 24 Healthcare Ltd.

Information Security Policies, Staff Policies & Procedures and terms and conditions which concern the confidentiality, integrity and availability of Vital 24 Healthcare Ltd information and which includes rules about acceptance use, breach reporting, IT monitoring and use of mobile devices.

ROLES AND RESPOSIBILITIES

A controller determines the purposes and means of processing personal data.

A processor is responsible for processing personal data on behalf of a controller.

Vital 24 Healthcare Ltd's Data Protection Officer, (currently the Company Director) is overall responsible for the documentation of this policy. This is then delegated to the Registered Manager for operational actions and requirements to ensure compliance.

If employees have any questions about data protection in general, this policy or their obligations under it, they should direct them to the Data Protection Officer and/or Vital 24 Healthcare Ltd's Business Directors.

Please see appendix for further information regarding Roles and Responsibilities.

DATA PROTECTION PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).
4. Accurate and where necessary, kept up to date (Accuracy).
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation).
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
7. Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
8. Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

PERSONAL DATA

Current legislation applies to “personal data” meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Legislation applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of annual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

SENSITIVE PERSONAL DATA

The GDPR refers to sensitive personal data as “special categories of personal data”. The special categories specifically include genetic data and biometric data, where processed to uniquely identify an individual.

Vital 24 Healthcare Ltd will not retain sensitive personal data without the express consent of the employee in question.

Vital 24 Healthcare Ltd will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles.

If Vital 24 Healthcare Ltd enters into discussions about a merger or acquisition with a third party, Vital 24 Healthcare Ltd will seek to protect employee’s data in accordance with the data protection principles.

Personal Data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

EMPLOYEE RIGHTS

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

LAWFUL BASES FOR PROCESSING

There are six available lawful bases for processing. No single basis is better or more important than the others – which basis is more appropriate to use will depend on the purpose and relationship between Vital 24 Healthcare Ltd and the individual.

At least one of these must apply when personal data is processed:

1. CONSENT: the individual has given clear consent in the application for employment for Vital 24 Healthcare Ltd to process their personal data for a specific purpose. The GDPR gives a specific right to withdraw consent. The individual has the right to withdraw.
2. CONTRACT: the processing is necessary for a contract Vital 24 Healthcare Ltd has with the individual, or because they have asked Vital 24 Healthcare Ltd to take specific steps before entering into a contract in their application for employment.
3. LEGAL OBLIGATION: the processing is necessary for Vital 24 Healthcare Ltd to comply with the law (not including contractual obligations).
4. VITAL INTERESTS: the process is necessary to protect someone's life.
5. PUBLIC TASK: the processing is necessary for Vital 24 Healthcare Ltd to perform a task in the public interest or for the agency's official functions, and the task or function has a clear basis in law.
6. LEGITIMATE INTERESTS: the process is necessary for Vital 24 Healthcare Ltd's 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.

DATA SUBJECT PRIVACY NOTICES

Vital 24 Healthcare Ltd will inform each individual:

1. Our intended purposes of processing personal data
2. The lawful basis for processing.

This applies whether Vital 24 Healthcare Ltd collect the personal data directly from the individual or collect from another data source.

DATA SUBJECTS ACCESS REQUESTS

An employee, person we support, or stakeholder has the right to access information kept about them at Vital 24 Healthcare Ltd.

The Data Protection Officer, along with the Business Directors are responsible for dealing with data subject access requests.

These requests can be made free of charge. However, we may charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Vital 24 Healthcare Ltd will respond to any data subject access request and provide the information within 1 month of the receipt.

Vital 24 Healthcare Ltd will be in a position to extend the period of compliance by a further 2 months where requests are complex or numerous. If this is the case, Vital 24 Healthcare must inform the individual within 1 month of the receipt of the request and explain why the extension is necessary.

Vital 24 Healthcare Ltd will allow individuals access to hard copies of any personal information. However, if this involves a disproportionate effort on the part of Vital 24 Healthcare Ltd, the individual will be invited to view the information on screen or inspect the original documentation at a place and time agreed by the agency.

CORRECTION, UPDATING AND DELETION OF DATA

Vital 24 Healthcare Ltd may monitor clients by various means, including but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, Vital 24 Healthcare Ltd will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about him/her.

Vital 24 Healthcare Ltd will not retain such data for any longer than is absolutely necessary.

EMPLOYEES' OBLIGATIONS REGARDING PERSONAL INFORMATION

If an employee acquires any personal information in the course of their duties, they must ensure that:

1. The information is accurate and up to date, insofar as it is practicable to do so.
2. The use of the information is necessary for a relevant purpose and that it is not kept longer than necessary.
3. The information is secure.

In particular an employee should always ensure that they:

1. Use password-protected and encrypted software for the transmission and receipt of emails
2. Lock files in a secure cabinet.

Where information is disposed of, employees should ensure that it is destroyed securely. This may involve the permanent removal of the information of the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an employee acquires any personal information in error by whatever means, they must inform the line manager/Data Protection Officer immediately and if it is not necessary for them to retain the information, arrange for it to be handled by the appropriate individual within Vital 24 Healthcare Ltd.

If an employee is in any doubt about what they may or may not do with personal information, they should seek advice from the line manager/the Data Protection Officer. If they cannot get in touch with the line manager or the Data Protection Officer, they should not disclose the information concerned and should await contact.

CONSEQUENCES OF NON-COMPLIANCE

Vital 24 Healthcare Ltd and all employees are under an obligation to ensure that they have regard to the data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action, up to and including dismissal. For example, if an employee accesses another employee's employment records, without the requisite authority, Vital 24 Healthcare Ltd will treat this as potential gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

TAKING CLIENT RECORDS OFF SITE

An employee must not take records off site (whether in electronic or paper format) without prior organisation from the Data Protection Officer or Senior Management.

Any employee taking records offsite must ensure that they do not leave their laptop (if applicable), other device or any hard copies of employment records on public transport, in vehicles or any public place. Care must be taken when observing information in hard copy or on-screen, that such information is not viewed by anyone who is not legitimately privy to that information.

THIRD PARTY SUPPLIERS AND SUBCONTRACTORS COMPLIANCE

Notices/statements will be sent to third parties who handle, have access to or process information on behalf of Vital 24 Healthcare Ltd. These statements should address the need to protect the organisation's data.

Vital 24 Healthcare Ltd will contractually require that sub-contractors review and comply with this policy.

APPENDICES

This policy has supplementary information. Please see appendices.

ADDITIONAL INFORMATION

Data Audit information is available on request.

Information regarding data storage and disposal is available on request.

WHERE TO GET HELP WITH THIS POLICY/PROCEDURE

Please contact the Data Protection Officer and/or Vital 24 Healthcare Ltd Business Directors.

COMPLIMENTS OR COMPLAINTS

Please contact the Data Protection Officer and/or Vital 24 Healthcare Ltd Business Directors.

Appendix 1

CONFIDENTIALITY POLICY

Agency workers will in the course of his/her employment have access to and be entrusted with trade secrets and information in respect of the business, administration and financing of the employment business and its dealings, transactions and affairs and its clients, staff and agency workers, whether or not contained in the databases of the agency or in the paper notes of the clients which information is or maybe confidential.

The agency worker may not (except in the proper course of his/her duties or unless ordered to do so by a court of jurisdiction) during or at any time after the agency workers assignments, divulge to any person, whatever or otherwise, make use of any confidential information and he/she shall use his/her best endeavours to prevent the improper use, disclosure or communication of confidential information.

Confidential information will be deemed to extend to all confidential technical and commercial information including, but not limited to the contents of reports, specifications, quotations, formulae, computer records, client lists, price schedules, clients and the like.

These restrictions above, shall not apply in respect of any information which either is or has become in the public domain (otherwise than by a breach of the agency worker of this clause) or which he/she is required to disclose by court or competent authority or which by virtue of the agency worker's assignments are part of his/her own skill and knowledge.

WHAT NOT TO DO:

1. The agency worker must not discuss the affairs of the employment business, clients or patients with anybody unless they have specific or verifiable permission to do so.
2. The agency workers must not purposely seek to obtain confidential information about the employment business, clients or patients outside of the strict scope of their job role.

WHAT YOU MUST DO:

1. The agency workers must always ask a Manager for advice if they are not certain about how to deal with possibly confidential information.
2. The agency workers must keep all information about the affairs of the employment business, clients or patients, strictly confidential.
3. The agency workers must always remember that the requirements of this policy are also requirements for undertaking assignments with the employment business.
4. The agency workers must always remember that the employment business will report the seemingly unauthorised spreading of information to clients and patients.
5. Exceptions: This policy does not apply to cases where the holder of information knows that the law or the regulations that they work under requires them to report that knowledge.

SERVICE USER'S PERSONAL DATA

Care worker, manager and office staff shall ensure that any personal information about a service user for whom a care worker is supplied by the agency, is not disclosed to any member of the agency's staff unless it is necessary to do so in order to provide an effective service to the service user.

The principles of confidentiality must be observed in discussion with colleagues and the manager, particularly when undertaking training or group supervision sessions.

This does not prevent workers discussing (where appropriate and not a breach of service user's confidentiality) with the service user, their families and friends, care worker, manager, and other caring professions ways to improve the quality of life enjoyed by the service user.

It also does not prevent disclosures that are appropriate where persons are at risk and the worker has a duty to report (as discussed in the previous section).

If a worker needs advice on how to deal with personal data, they should contact the duty manager.

CARE WORKER'S PERSONAL DATA

Vital 24 Healthcare Ltd will hold computer records and personnel files relating to the agency workers.

These will include the agency workers' employment application, references, bank details, performance appraisals, holiday and sickness records, remuneration details and other records, (which may include data relating to the agency workers health and data held for monitoring purposes).

The employment business requires such personal data for personnel, administration and management purposes and to comply with its obligations regarding the keeping of personal records.

The agency workers right of access to this data is as prescribed by law.

In terms of the agency workers contract, the employment business may process personal data of an agency worker relating for personnel, administration and management purposes (including data relating to the agency workers health and data held for monitoring purposes) and may, when necessary for those purposes, make such data available to its advisors, to parties providing products and/or services to the employment business (including, without limitation, IT systems suppliers, pension benefits and payroll administrators), to regulatory authorities, to any potential purchasers of the company or its business (on a confidential basis) and as required by law.

The employment business may transfer such data to and from Group Companies.

The employment business may, in terms of the agency workers contract, handle, process and divulge such information as may be necessary for the company or its agents to perform its business or duties.