Data Protection Policy

V2.0 October 2025

Document Information

Document Title	Data Protection Policy
Reference	OT Service DP Policy
Version	2.0
Author	Stamatoula Kaditi
Owner	The Occupational Therapy Service
Approved by	Lucy Leonard (Director)
Approval date	31st October 2025
Issue date	6th October 2025

Related Documents

Reference	Title	Owner
OT Service IS Policy	Information Security Policy	The Occupational Therapy Service

1. Introduction

The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 imposes certain obligations upon "the Company" in relation to the processing of personal data. These obligations are contained within six data protection principles. The Company and all staff including employees, associates, temporary workers and volunteers, agency workers, contractors, job applicants must always comply with these principles in their information handling practices.

2. Key Definitions:

- 'Data subjects' means individuals about whom we process personal data
- 'Personal data' means data which relate to a living individual who can be identified from those data or from those data and other information,
- 'Processing' means any operation performed on personal data including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction.
- 'Special category data' means personal data about an individual's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; biometric and genetic data; membership of a trade union; physical or mental health or condition; sexual life; commission or alleged commission of an offence; or the proceedings relating to any alleged or actual offences, the disposal of such proceedings or the sentence of the court in such proceedings
- 'Controller' means The Company, which determines the purposes and means of processing personal data.

3. The UK GDPR Principles:

3.1 The Company's policy is to respect the privacy of individuals when processing their personal and private information, to comply with its statutory and other obligations regarding individual privacy, and also to observe the guiding principles underlying those obligations, which may be summarised as:

3.2 Processing data fairly and lawfully and to meet this obligation the Company must ensure that the processing satisfies certain conditions in relation to personal data and additional conditions in relation to sensitive data. The key pre-conditions are that the data subject has given their consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive data may only be processed with explicit consent of the data subject.

3.3 Making sure that data is obtained only for one or more specified and lawful purposes, and that it is not processed in any manner incompatible with those purposes.

3.4 Making sure that data is adequate, relevant and not excessive in relation to the purposes for which it is processed.

3.5 Making sure personal data is accurate and where necessary up to date.

3.6 Keeping personal data for no longer than is necessary.

3.7 Processing in accordance with the data subject rights under the Act.

3.8 Keeping personal data secure against loss or misuse.

3.9 Not transferring data to a country or territory outside the UK European Economic Area unless that country or territory ensures adequate level of protection to the processing of personal data. Standard contractual clauses or binding corporate rules.

4. The Company Policy with Regard to Employees and Associates

4.1 The Company processes personal data about current and former job applicants (successful and unsuccessful), and current and former employees, agency staff, casual staff and contract staff including associates. This policy applies to all such data and parts of it also apply to others in the workplace, such as volunteers, vacation students and those on work experience.

4.2 The Company processes employee and Associate personal data for a number of specific purposes in relation to their employment or engagement. Data processing is undertaken by the Company for a range of purposes, including personnel, administrative, financial, regulatory, payroll and business development, including possible disposals of the whole or parts of the business or the acquisition of new businesses. Where individuals are (or have expressed an interest in) receiving benefits or services from an external provider, relevant data is disclosed to them too. All processing is carried out in accordance with the Act.

4.3 The Company will review employees and Associates files on a regular basis to ensure they do not contain a backlog of out of date or irrelevant information and to check there is a sound business reason requiring information to continue to be held.I

4.4 If your personal information changes, for example you change address or you get married and change your surname, you must inform the Company as soon as practicable so that the Company's records can be

4.5 Retention periods are documented and based on legal regulatory and operational needs. For example, unsuccessful job applicant data retained for up to 12 months. Data no longer required will be securely deleted or anonymised.

4.6 The Company implements appropriate technical and organisational measures to safeguard personal data:

- Physical security (e.g. locked cabinets)
- Digital security (e.g. password protection, encryption)
- Access controls and staff training
- Secure backup and recovery procedures

4.7 Please note that amongst the data subject rights set out in the UK GDPR, data subjects are entitled:

- to be informed about data collection and use,
- to access their personal data,
- for rectification inaccurate or incomplete data,
- to erase personal data,
- to restrict processing,
- to data portability,
- to object to processing,
- to not be subject to automated decision-making and profiling without meaningful human involvement.

4.8 Requests can be made by contacting Data Protection Officer. Access to personal data is provided free of charge unless requests are excessive or unfounded.

5. Your Responsibilities as an Employee or Associate

5.1 You must familiarise yourself with this policy and implement its requirements within your working practices. Pursuant to the terms of your employment or Associates agreement with the Company you have an obligation to comply with this policy.

ANY FAILURE TO COMPLY WITH THIS POLICY MAY BE A BREACH OF CONTRACT. NEGLIGENT OR DELIBERATE BREACHES MAY RESULT IN DISCIPLINARY ACTION AND IN SOME CASES, LEGAL CONSEQUENCES.

5.2 During the course of your work, you will come into contact with or use confidential information about employees, associates, clients and suppliers. The purpose of this policy is to ensure that you do not breach the Act. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from A company Director, or the Company data protection officer. You must ensure you comply with the following guidelines at all times:

- Do not give out confidential personal information except to the data subject. It should not be given to someone either accidentally or otherwise, from the same family or to any unauthorised third party unless the data subject has given their explicit consent.
- Always verify the identity of the data subject and the legitimacy of any request before releasing any personal information by telephone.
- Only transmit personal information between locations by secure encrypted communication channels or email if a secure network is in place.
- Ensure that any data that you hold is kept securely.

6. Data Security

6.1 UK GDPR requires appropriate technical and organizational measures to ensure data security and requires us to take appropriate technical and organisational measures to safeguard personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.

6.2 We recognise the importance of personal data to our business and the importance of privacy rights to individuals about whom we process personal data. This policy is not limited to protecting personal data but extends to all information which we hold. References to ‘personal data’ should be read to include information of any kind that is used within the business, including confidential information.

6.3 In order to assist us to comply with the seventh principle:

- You must comply with the technical and organisational measures set out in appendix 1 to this policy whenever you process personal data
- You must consider the nature of the personal data you are processing and determine whether the technical and/or organisational measures are commensurate to the harm that might result if there were a security breach. If the data are also confidential or sensitive personal data, an additional level of security will be required:

(a) Examples of confidential information may include (HR data (e.g. employee records, payroll data); financial information (e.g. bank account and/or credit card details);

(b) Examples of sensitive personal data may include information about an individual's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; membership of a trade union; physical or mental health or condition; sexual life; commission or alleged commission of an offence; or the proceedings relating to any alleged or actual offences, the disposal of such proceedings or the sentence of the court in such proceedings);

- You should only hold personal data for as long as it is required for the purpose for which those data were originally collected. Once the data are no longer required, you must destroy or delete those data securely
- You must immediately report all actual or suspected security breaches to the Data Protection officer at dpa.officer@oaklandgrp.com, or a company Director.

5.2 The Company is responsible for taking reasonable steps to ensure the reliability of associates and staff that have access to personal data. If you are responsible for the recruitment of staff (whether permanent, temporary or contract), you must assist us to comply with this requirement by:

- screening/vetting all new staff
- ensuring all new staff sign terms and conditions which include confidentiality and security obligations
- taking up references for all new staff
- ensuring new staff are trained on the care and handling of personal data when they joint (e.g. as part of their induction training).

7. Contracts and Responsibilities

7.1 If you have any queries about this Policy, please contact A company Director.
7.2 We reserve the right to change this Policy from time to time to take into account any relevant changes in law or guidance from the Information Commissioner. Updates will be communicated to staff and documented with version control.

7.3 Technical and Organisational Measures

The Company has in place the following technical and organisational measures to ensure compliance with the Act. Any references to data within this Appendix includes all data held in relation to the Company and its clients and includes personal and sensitive data within the meaning of the Act. All employees, staff and associates are required to use and implement these measures in their working practices:

7.4 Technical Security Measures

- Installation of protection against malicious software/viruses. Software should not be installed from removable media or downloaded from the internet without virus checking it first.
- Backing up data – regular backups of all data on computer systems; data should not be stored on local drives or removable media as these will not be backed up).
- Encryption of all Company related matters.
- Secure exchanges of information.

- User access controls (e.g. computers are to be password protected; passwords should be changed on a regular basis; passwords should not be pinned up next to the computer or anywhere else where they could be seen; passwords should include a mixture of letters and numbers; avoid passwords that are easy to guess such as your name or date of birth; if using shared/family pc you must store your work under a separate password protected file).
- In the event of mobile computing laptops or other personal computing items should not be left unattended in cars or in public places or on top of desks left unattended overnight.
- If using a home/shared computer, then you must ensure that appropriate measures are taken to ensure that data kept on that computer is secure including the steps set out in 1 to 6 above.
- Disaster recovery (e.g. ensure copies of personal data are stored off site in a secure and fire-proof location; business continuity plan should be created; disaster recovery and business continuity plans should be tested periodically).
- Secure destruction or deletion of data and secure disposal of computer equipment and removable media (e.g. where you are destroying personal data or confidential information make sure that you do so securely by using a high spec shredder or confidential waste disposal agent; make sure that all hard drives are erased on all computers before their disposal).

APPENDIX 1

Organisational Security Measures

1. Positioning equipment so as to prevent screens from being overlooked (e.g. make sure that any personal data displayed on computer screens cannot be overlooked by passers-by).
2. Securing equipment.
3. Secure disposals of equipment or its re-use/re-conditioning.
4. Clear desk and clear screens policies to be implemented by all Associates.
5. Paper data should be kept in a lockable, fireproof filing cabinet with access keys stored reasonably and with restricted access.
6. Any data relating to Company matters when mobile should keep in a lockable bag, it should not be left unattended in the car or otherwise.
7. Associates must report actual or suspected breaches of the Company security measures and Data Protection Policy to A company Director immediately.
8. Training – Associates should ensure they keep themselves up to date with the current statutory and professional obligations with regard to data protection and confidentiality. (e.g. on the care and handling of personal data; on security systems; on the procedure for handling security breaches). U.K. GDPR training awareness is mandatory and recurring with records of completion.