Data Protection Policy (Client)

1. Purpose and Scope

This policy applies to the collection, use and storage of client and customer (termed 'clients' throughout this Policy) data, including personal data, within manual and electronic records kept by the Company in connection with its service provision function as described below. It also covers the Company's response to any data breach and other rights under the UK's Data Protection Act, and General Data Protection Regulations.

Data Protection Act 2018 (DPA 2018)

The DPA 2018 is the UK's implementation of the European Union's General Data Protection Regulations (GDPR) following the UK's exit from the EU. The DPA controls how to protect client's data taken, used and stored by the Company.

UK General Data Protection Regulations (UK GDPR)

The EU GDPR is an European Union Regulation and no longer applies to the UK. As a business, if we operate only in the UK, we need to comply with the DPA 2018. However, the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR, with the core data protection principles, rights and obligations being broadly similar.

Legally, data processors located in the EU and EEA are able to send client/personal data to and from UK controllers with no restrictions due to the EU having had an 'approved adequacy' decision for the UK (i.e. an 'essentially equivalent' level of data protection). This decision is currently in place until the 27 June 2025, following which a review of this policy will be necessary.

As of January 2021, businesses in the UK have had to ensure they consider **both** legal contexts – the DPA 2018, and the UK GDPR – in relation to data protection. Both are linked below for ease:

Data Protection Act 2018
UK General Data Protection Regulations 2018

Company Overview

Osprey Academy is the sister concern of St. John's group of institutions, which has more than 30 years of experience in nursing field, including the training and education of more than 20,000 nurses. Most of the students are working in the UK, USA, Canada, Australia, New Zealand, Dubai, Asia, Europe and India. Osprey Academy transforms regionally trained nurses to global nurses by advancing their nursing knowledge and skills, and by introducing them to study and work opportunities across the globe. We provide end to end solution for overseas training and work related needs.

This policy applies to the data of perspective visa applicants including those of the organisations or bodies connected in the recruitment of applicants. These are referred to in this policy as relevant individuals and/or clients.

For the benefit of doubt, this policy relates to data protection requirements within the UK, and in line with 'approved adequacy' for data processing within the EU (27 member states) and EEA (30 member states, plus Switzerland) – full list HERE.

Client/Personal Data
This is information that relates to an identifiable individual who can be directly or indirectly identified from that information, i.e. a person's name, identification number, location, online identifier. It can also include pseudonymised data.

Special Categories of Personal Data
This is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

Criminal Offence Data
This is data which relates to an individual's criminal convictions and offences.

Data Processing
Any operation or set of operations which is performed on client data or on sets of client data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Company makes a commitment to ensuring that client/personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with the DPA 2018, UK GDPR and domestic laws, and all its clients should conduct themselves in line with this.

Where our service also incorporates a third parties processing data on behalf of the Company, we will ensure that the third party takes such measures in order to maintain the Company's commitment to protecting data. In line with current data protection legislation, the Company understands that it will be accountable for the processing, management and regulation, and storage and retention of all client/personal data held in the form digital records and on computers.

Types of Data Held
Client data and records are kept in files or folders stored on the Company's electronic storage system. The following types of data may be held by the Company, as appropriate, on relevant clients:

- Name, address, email, phone numbers – for individual and emergency contacts.
- CVs and other information gathered during recruitment.

- References from former employers.
- Previous job titles, job descriptions and pay grades.
- National Insurance number(s) and Tax code(s).
- Medical or health information.
- Training and education records.
- Terms and conditions of employment and/or placement.
- Identification documentation (ID).
- Right to Work confirmation.
- Visa details to include qualifications.

2. Data Protection Principles

All client's personal data obtained and held by the Company will:

- Be processed fairly, lawfully and in a transparent manner.
- Be collected for specific, explicit, and legitimate purposes.
- Be adequate, relevant and limited to what is necessary for the purposes of processing.
- Be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
- Not be kept for longer than is necessary for its given purpose.
- Be processed in a manner that ensures appropriate security of client/personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.
- Comply with the relevant data protection procedures for international transferring of client/personal data.

In addition, client/personal data will be processed in recognition of an individuals' data protection rights, as follows:

- The right to be informed.
- The right of access.
- The right for any inaccuracies to be corrected (rectification).
- The right to have information deleted (erasure).
- The right to restrict the processing of the data.
- The right to portability.
- The right to object to the inclusion of any information.
- The right to regulate automated decision-making and profiling of personal data.

3. Procedures

The Company has taken the following steps to protect the client data of relevant individuals, which it holds or to which it has access:

- It has registered with the Information Commissioner's Office (ICO) due to legal requirements of processing personal data.

- The Company's website contains details of our **Privacy Policy** – click HERE.

- The Company appoints or employs individuals with specific responsibilities for the following, additionally, there are clear lines of responsibility and accountability for these roles:

  a) The processing and controlling of data.
  b) The comprehensive reviewing and auditing of its data protection systems and procedures.
  c) Overviewing the effectiveness and integrity of all the data that must be protected.

- The Company provides information to its clients on their data protection rights, how it uses their personal data, and how we protect it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.

- The Company can account for all client/personal data it holds, where it comes from, who it is shared with and also who it might be shared with.

- The Company carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its client/personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of client/personal data in and by the Company.

- The Company recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their client/personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Company understands that consent must be freely given, specific, informed and unambiguous. The Company will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.

- The Company has the appropriate mechanisms for detecting, reporting and investigating suspected or actual client/personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioners Office (ICO), and is aware of the possible consequences.

- It is aware of the implications and penalties that could result from client/personal data held within the UK being transferred internationally against the DPA 2018 and UK GDPR. More details on international transfer of data is available from the ICO.

Access to Data
Relevant individuals have a right to be informed whether the Company processes client/personal data relating to them and to access the data that the Company holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- A form on which to make a subject access request is available from **Dr Vimal Sudakar**. The request should be made to **drvimal@osprey-academy.com**.

- The Company will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request.

- The Company will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within **one month** as a maximum. This may be extended by a further **two months** where requests are complex or numerous.

Relevant individuals must inform the Company immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Company will take immediate steps to rectify the information. For further information on making a subject access request, clients should refer to our subject access request policy, available from **Dr Vimal Sudakar**.

Data Disclosures
The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- Any client-related benefits operated by third parties.
- Individuals with disabilities – whether any reasonable adjustments are required to assist them at work or within their studies.
- Information relating to Right to Work and/or Visa confirmations.
- Individuals' health data – to comply with health and safety or occupational health obligations towards the client, and in terms of consideration as to how the individual's health could affects their ability to become employed and/or study.
- Data as requested by a UK government department or agency, such as the HMRC.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security
The Company adopts procedures designed to maintain the security of data when it is stored and transported. More information can be requested from **Dr Vimal Sudakar** concerning data transfer security. In addition, employees of Osprey Academy must:

- Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people.
- Refrain from sending emails containing sensitive work related information to their personal email address.
- Check regularly on the accuracy of data being entered into computers.
- Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
- Use computer screen blanking to ensure that client/personal data is not left on screen when not in use.

Client/personal data should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by **Dr Vimal Sudakar**. Where client/personal data is recorded on any such device it should be protected by:

- Ensuring that data is recorded on such devices only where absolutely necessary.
- Using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
- Ensuring that laptops or USB drives are not left lying around where they can be stolen.

All employees who need to use the computer system are trained to protect clients/individuals' personal data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

Should an employee of Osprey Academy fail to follow the Company's rules on data security, this will be dealt with via the Company's Disciplinary Policy.

International Data Transfers

The Company does not transfer client data to any recipients outside of the EEA. In light of the Company operating within both UK (London) and India (Chennai, Kochi and Vellore), this is not considered to be a 'restricted transfer', as the sharing of personal data will be with a UK based company and its processor, located in India only.

Breach Notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the ICO within 72 hours of the Company becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual. If the breach is sufficient to warrant notification to the public, the Company will do so without undue delay.

Data Protection Officer
The Company's Data Protection Officer is **Dr Vimal Sudakar**, who can be contacted at drvimal@osprey-academy.com. The nominated DPO is trained appropriately in their role in relation to data protection legislation.

Records
The Company keeps records of its processing activities including the purpose for the processing, and retention periods as required. These records will be kept up to date so that they reflect current processing activities.

4. Monitoring and Review

The Director is responsible for monitoring that clients are adhering to this policy and the procedures contained within. Should there be any query about the responsibilities or processes involved within this policy, the Manager should be approached in the first instance, escalating to the Director as required.

This policy will be reviewed in June 2025, in line with legislative updates regarding the UK and EU having 'approved adequacy', as detailed in Section 1, or before this date should legislation, regulation or good practice guidance requires changes.

Last review: February 2024
Next review: June 2025