Policy and Procedure
Information Governance and Data Protection Policy

1. Introduction

1.1 This Data Protection Policy is the overarching policy for data security and protection for Joubert Consulting Ltd (hereafter referred to as "us", "we", or "our").

2. Purpose

2.1 The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the UK General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

2.2 This policy covers:

2.2.1 Our data protection principles and commitment to common law and legislative compliance;

2.2.2 procedures for data protection by design and by default.

2.2.3 All NHS bodies, and Independent organisations who deliver NHS services, has a legal duty to keep information about patients and service users confidential.

3. Scope

3.1 This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

3.2 This policy applies to all staff, including temporary staff and contractors.

4. Principles

4.1 We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.

4.2 We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation. The principle of Confidentiality is underpinned by our Confidentiality policy.

4.3 We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent.

4.4 Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Policy: Consent to examination or assessment. We ensure that it is as easy to withdraw as to give consent.

4.5 We will undertake annual audits of our compliance with legal requirements.

4.6 We acknowledge our accountability in ensuring that personal data shall be:

4.7 Processed lawfully, fairly and in a transparent manner;

4.8 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.9 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4.10 Accurate and kept up to date;

4.11 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

4.12 Processed in a manner that ensures appropriate security of the personal data.

4.13 We uphold the personal data rights outlined in the UK-GDPR:

4.14 The right to be informed;

4.15 The right of access;

4.16 The right to rectification;

4.17 The right to erasure;

4.18 The right to restrict processing;

4.19 The right to data portability;

4.20 The right to object;

4.21 Rights in relation to automated decision making and profiling.

4.22 In line with legislation, we employ a nominated Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

4.23 We complete the Data Security and Protection Toolkit on an annual basis and our publication status can be found here: https://www.dsptoolkit.nhs.uk/OrganisationSearch

4.24 Identifiable information will only be shared when there exists a fair and lawful basis, as set out by the NHS Care Record Guarantee and NHS Constitution.

5. Sharing of Data

5.1 The NHS Care Record Guarantee and NHS Constitution provide a commitment that all NHS organisations and those providing care on behalf of the NHS, will use records about patients and service users in ways that respect their rights and support their health and wellbeing.

5.2 We may share anonymised with other NHS and social care partner agencies for the purpose of improving local services, research, audit and public health.

5.3 As per 4.24, we only share information that identifies individuals when we have a fair and lawful basis; this includes, but is not limited to, the following:

- 5.3.1 For the purposes of the provision of health or social care or treatment or the management of health or social care systems.
- 5.3.2 When we are lawfully required to report certain information to the appropriate authorities e.g. to prevent fraud or a serious crime.
- 5.3.3 To protect children and vulnerable adults.
- 5.3.4 When an individual has given us permission.
- 5.3.5 When a formal court order has been served.
- 5.3.6 Emergency planning reasons such as for protecting the health and safety of others.
- 5.3.7 When permission is given by the Secretary of State or the Health Research Authority to process confidential information without the explicit consent of individuals.

5.4 We will only share and use the minimum amount of information necessary is perform our duties.

6. Data protection by design and by default

6.1 We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

6.2 We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

6.3 It is unlikely that any small organisation will be required to undertake a data protection impact assessment. Though it is considered best practice to do one for your care plans at a minimum. Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist.

6.4 All new systems used for data processing will have data protection built in from the beginning of the system change.

6.5 All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

6.6 We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

6.7 In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

6.8 Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

7. Responsibilities

7.1 Our designated Data Security and Protection Lead is **Lesia Joubert**. The key responsibilities of the lead are:

7.2 To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles;

7.3 To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.

7.4 To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT.

7.5 To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management and DPO to fulfil this work.

7.6 Our designated DPO is Lesia Joubert, they can be contacted via email: lesia@neurodiversityassessment.com; phone: 07968751304*;* or at the following address: C/O O'Meara Fitzmaurice & Co, Brimstage Hall, Brimstage Road, Wirral, United Kingdom, CH63 6JA

7.7 The key responsibilities of the DPO are:

7.8 Overseeing changes to systems and processes;

7.9 Monitoring compliance with the UK-GDPR and the Data Protection Act 2018;

7.10 Completing DPIA;

7.11 Reporting on data protection and compliance with legislation to senior management;

7.12 Liaising, if required, with the Information Commissioner's Office (ICO).

8. Approval

8.1 This policy has been approved by the undersigned and will be reviewed annually.

Name	Lesia Joubert
Signature	*Lesia Joubert*
Approval Date	01/11/2024
Review Date	01/11/2025