DATA PROTECTION POLICY

The Data Protection Act 2018 is the UK version of EU regulations called the General Data Protection Regulations (GDPR). As the principles of the changes to data protection legislation are in UK law (introduced 25th May 2018), they still apply after the UK has left the EU.

The PJL Data Protection Policy affects how PJL Healthcare Ltd manages personal data of staff, residents and other people/organisations it collects data about. It affects what data we can ask you to give us, how we store it, how we protect it, when we have to delete it, how quickly we have to respond if someone wants to see all of the personal data that we store about them, the circumstances under which we are allowed to share it and telling you if we do share your data. It makes sure that personal data that goes through a new technology is as well protected as data in old technologies or as well as the data stored as printed sheets in a filing cabinet. It introduces tougher fines for non-compliance and breaches, and it gives people the right to choose some aspects of what organisations can do with their data.

DATA PROTECTION OFFICER

The company has appointed Mr Paul Sellars as Data Protection Officer whose details are shown below:

Email: paul.sellars@pjlhealthcare.co.uk
Telephone: 01435 872201

ICO REGISTRATION

PJL Healthcare Ltd are registered with the information commissioner's office (ICO).

Certificate Reference Number: Z1321501

PRIVACY NOTICES

The list of Privacy Notices we hold are listed below. A Privacy Notice is a generalised statement of what data we collect and hold about you. It also contains the legal reasons why we are allowed to hold that data and the reasons why we have to share some of that data. In addition, if you have given consent for photography/digital images, it tells you what these are used for and what your legal rights are:

- Job Applicants Privacy Notice.
- Staff Privacy Notice.
- Ex-Staff Privacy Notice.
- Children and Young People Privacy Notice.
- Visitors Privacy Notice.
- Website Privacy Notice.

Last updated 30 June 2021

DATA PROTECTION POLICY

DATA RETENTION SCHEDULE

To see the data retention periods for personal data, please see the Data Retention Schedule.

INDIVIDUAL RIGHTS REQUESTS

To make an individual rights request, please use the form:

• Individual Rights Request Form

Please send your completed form to:
paul.sellars@pjlhealthcare.co.uk

SUBJECT ACCESS REQUESTS

To make a subject Access Request, please use the form:

• Subject Access Request Form

Please send your completed form to
paul.sellars@pjlhealthcare.co.uk

DATA BREACH PROCEDURE

PJL Healthcare Ltd has robust controls in place for preventing data breaches and for managing them in the rare event that they might occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below.

1. Breach Monitoring & Reporting

The Company has appointed a Data Protection Officer DPO who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect.

2. Assessment of Risk and Investigation

The DPO ascertains what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches looking at:

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.g. encryption)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

3. Breach Recording

The Company utilises a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. The Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and record purposes. If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements.

The appointed lead will keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions. All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of 6 years from the date of the incident.

Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee held. A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the Company's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause. Resultant employee outcomes of such an investigation can include, but are not limited to:

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning (in-line with the Company's disciplinary procedures)

System Error

Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the DPO to assess the risk and investigate the root cause of the breach. Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause.

Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident:

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system

• Removing an employee from their tasks
• The use of back-ups to restore lost, damaged or stolen information
• If the incident involves any entry codes or passwords, then these codes must be changed immediately, and members of staff informed

4. Breach notification

The Company recognises our obligation and a duty to report data breaches in certain instances.

ICO Notification

The ICO is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, it would lead to significant detrimental effects on the individual. Where applicable, the ICO is notified of the breach no later than 72 hours of the reported breach and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes. If for any reason it is not possible to notify the ICO of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay.

Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the ICO in accordance with Article 33 of the GDPR.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include:
• The nature of the personal data breach
• The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information)
• A description of the likely consequences of the personal data breach
• A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)