jrhsupport

BRING YOUR OWN DEVICE POLICY

BRING YOUR OWN DEVICE POLICY

1. Introduction

1.1 This Bring Your Own Device Policy (BOYD) is JRH Support's policy regarding the safe use of personal smart phones for work-related purposes by our support staff.

1.2 Staff employed in administrative and managerial roles within the company are provided with alternative means to access personal data, such as computer systems and work smart phones.

1.3 Modern smart phones are capable of accessing and storing data and running business applications. While the use of smart phones can bring many benefits, they also introduce a significant risk. That risk is that personal data, or access to that data, may fall into the wrong hands due to the loss or improper use of a smart phone.

1.4 As an organisation we have taken a decision to allow support staff to use their own smart phones for work purposes. This policy has been developed to ensure that personal data held by the organisation is not put at risk from the use of smart phones in this manner. For those members of staff with a business requirement to access personal data with their own smart phone, this policy provides the necessary guidance so that it is done in a manner that does not introduce unacceptable threats to the safety and integrity of this data.

2. Purpose

The purpose of this policy is to:

2.1 Provide effective controls to ensure that support staff's access to personal data through the use of their own smartphone is authorised, secure and confidential, in line with our business requirements.

2.2 Ensure the remote processing of personal data is operated in accordance with statutory requirements and all relevant guidance.

2.3 Ensure that any risks associated with smart phone based access are recognised, assessed and managed.

3. Scope

3.1 This policy applies to all support staff employed by JRH Support.

4. Definitions

Personal Data – Information that relates to an identified or identifiable individual, as defined by the Data Protection Act 2018 and the GDPR

Smart Phones - A mobile phone that allows users to store information, use email and install programs (apps)

Support Staff – Persons employed by JRH Support who provide direct care and support to service users.

Service User – An individual who is provided care and/or support services by JRH Support.

5. Smart Phone Access Authorisation

5.1 Once recruited, all support staff will be required to download the Access Care Planning app from Google Play or App Store. Once downloaded, support staff will be required to register their smart phone with our admin department and be issued with a username and PIN to enable them to access relevant personal data on the app.

5.2 Support staff will only be able to access personal data using the Access Care Planning app with the device that is registered to them, and by inputting their personal username and PIN. There is no way that support staff can access personal data other than by using the app.

5.3 Support staff will only be able to use the Access Care Planning app to access the personal data of the service users they are directly supporting.

5.4 The Access Care Planning software will automatically download the relevant personal data of a service user to the staff member's app prior to the support visit taking place.

5.5 The Access Care Planning software will automatically remove the personal data of the service user from the staff member's app after the visit has been completed.

5.6 Support staff are not able to download any personal data to their device by using the Access Care Planning app.

5.7 When support staff leave JRH Support their device is deactivated as part of the employment termination process. This prevents further access to the Access Care Planning app.

6. Support Staff Responsibilities for the Security of Smart Phones

6.1 Support staff must not deliberately put their authorised smart phone at undue risk of being stolen, lost or accessed by unauthorised persons.

6.2 Support staff must report lost or stolen smart phones to their line manager as soon as possible. They should then notify our admin team by emailing hr@jrhsupport.co.uk. Our admin team will deactivate the smart phone and activate any replacement smart phone.

7. Support Staff Responsibilities for the Security of Personal Data

7.1 Service user's personal data can only be accessed by support staff using the Access Care Planning app.

7.2 Support staff are responsible for ensuring that unauthorised individuals are not able to see or access our data or systems via their registered smart phone. Smart phone screens should be locked when not actively being used.

7.3 The use of smart phones for accessing personal data in a public area should be kept to an absolute minimum, due to the risk of information being viewed or the theft of an unlocked device.

7.4 Emails containing personal confidential data and other confidential information must not be sent to or from personal email accounts.

Paul Battershall
General Manager