Beyond Limits Dumfries & Galloway provides policies and procedures to promote safe and consistent practice across the Organisation. The framework laid down within our policies and procedures lets everyone know how we work and reflects our values and mission statement. Our policies and procedures are written to help us, employees of Beyond Limits Dumfries & Galloway, to make good, safe decisions.

Beyond Limits Dumfries & Galloway expects all employees to be familiar with the contents of all policies and procedures relevant to their role and to understand how to apply them within their daily work.

None of these documents stand alone, all fit within the larger framework of how we work and any associated policies which are particularly relevant will be directly referenced.

Smart Phone Policy

Smart Phone – what this means to Beyond Limits Dumfries & Galloway

Beyond Limits Dumfries & Galloway recognises that modern smart phones are capable of accessing and storing data and running business applications. While the use of smart phones can bring many benefits, and help staff to do their jobs, it also introduces a significant risk. That risk is that data, or access to that data, may fall into the wrong hands due to the loss or improper use of a smart phone.

This policy has been developed to ensure that this organisation's data is not put at risk from the use of smart phones. For those members of staff with a business requirement to access the organisation's data with a 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.

The purpose of this policy is to:

- Provide effective controls to ensure that our staff's access to our data and any information systems using a smart phone is authorised, secure and confidential and in line with the business requirements of Beyond Limits Dumfries & Galloway.

- Ensure the remote processing of our data is in accordance with statutory requirements and all other relevant guidance.
- Ensure that any risks associated with smart phone-based access are recognised, assessed and managed.

Smart Phones on Issue

- Beyond Limits in Plymouth maintains a log of all smart phones issued in their information Asset Register.
- All smart phones issued will be installed with the appropriate and approved encryption and PIN control.
- Users must return all smart phones to the Service Leader when access is no longer required or when leaving the organisation. All data from returned devices will be deleted or archived and the device reset and wiped.

User Responsibilities for the Security of Smart Phones

- All smart phones should be held and transported securely and should not be left unattended, for example in vehicles, and should be locked away when not in use.

Stolen or lost equipment must be reported as soon as possible to the Plymouth Office on 01752 546449 or info@beyondlimits-uk.org.

Users must not install any unauthorised or unlicenced software on any of Beyond Limits Dumfries & Galloway smart phones.

Issued smart phones must only be used by the individual that they have been issued to. A user may not share the device with, or lend it to anyone else, for example a family member or work colleague.

User Responsibility for the Security of Personal Confidential Data and Information

Our data should only be remotely accessed, held and processed on smart phones supplied or authorised by Beyond Limits Dumfries & Galloway.

Users are responsible for ensuring that unauthorised individuals are not able to see or access our data or systems. Smart phones should not be shared with any other person, even for temporary access to a non-work-related app or service. Smart phone screen should be locked when not actively being used.

The use of smart phones in a public area should be kept to an absolute minimum due to the risk of information being viewed and the theft of equipment.

Staff must ensure that Beyond Limits Dumfries & Galloway smart phones and information accessed at home are secure from theft and damage and cannot be accessed by family members, friends or any other unauthorised user.

Data should not be held on a smart phone for longer than it is required and should be deleted or archived promptly to reduce the risk of the data being accessed by the wrong person.

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

User Responsibility for the Use of Personal Smart Phones

Users will not use personal smart phones to access our services or data unless written permission is given by the Finance Director and you will be asked to follow our Bring Your Own Device Policy.

Reporting Security Incidents and Weaknesses

Staff are responsible for smart phones and all data held on them. In the event of loss, theft or any data security incidents associated with smart phone use, users must report to the Beyond Limits Plymouth office on 01752 546449 and follow the data breach procedures in our Data Security Policy.

Our network administrators will then wipe any data on the handset and bar all calls.