

mobile device management



bring your own device

If your company is already operating with employees using their own devices, our MDM solution for BYOD allows this to continue.

It will give your company the ability to control the business content employees receive and add additional layers of data protection that will support your GDPR policy and prevent 3rd party data sharing.

With the workforce becoming progressively more 'mobile', the demand to access corporate data on-the-go is becoming increasingly vital, as is equipment and technology to make this possible, mobile technology is essential to running any business. Email, CRM and Support Systems apps are readily available for your team, increasing productivity as they are always connected. MDM ensures the protection of the data in these apps whilst making sure everyone on the team is running the correct secure version.



frontier mobile



 **frontiergroup**

BYOD controls

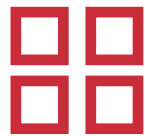


Our MDM solution for BYOD enables your business to control four major areas:



corporate email

Allowing you to push and remove corporate email to all of your devices via your Mobile Device Management portal



managed apps

Push business-critical applications and also remove them if a user leaves the organisation



content library

Push business-critical content to devices in a secure location. Set rules for this content so users cannot copy, paste or share files



password protection

Enforce passwords on BYOD devices to enhance the security of the entire device, keeping your corporate data safe and secure.

As we are experts in handling both Apple iOS and Android systems, we are ready to support whatever device your team is currently using