POLICY

Bring your own device (BYOD) policy for mobile phones (CP.017)

VGC Value – "We deliver on our promise" - We find solutions

Vision

Empowering our workforce through flexible technology choices, our BYOD policy endeavours to foster innovation, efficiency, and work-life balance. While embracing the future of work, we remain steadfast in safeguarding our VGC's data and maintaining the highest standards of digital security.

Strategy

This BYOD policy outlines the rules, standards, and procedures for staff whose roles have been identified as -

- Requiring a mobile phone for business use ***and***
- Require access to VGC IT resources, data, and networks ***and***
- Will use their personal mobile device for this purpose

Staff are permitted to use their personal mobile phones for work purposes, provided they comply with this policy.

Only smartphones and tablets that meet a minimum standard of security features (E.g. password protection, device encryption) and are able to install and execute Microsoft One Drive, Authenticator, Outlook, and Office 365 apps are eligible.

User Responsibilities

- Device Management: Mobile phone owners are entirely responsible for the management, maintenance, and updating of their devices.
- Security: Users must enable encryption and device-level password protection with a strong password and keep their operating systems and apps updated.
- Lost/Stolen Devices: In case of a lost or stolen device, the user must report the incident to the IT department as soon as they become aware via Artemis so that IT can close down access to VGC data systems. The user must ensure that a replacement device is provided within 24 hours. We recommend holding appropriate levels of insurance to cover this.
- Backup: Users should back up their personal data. VGC is not responsible for the loss of personal data.

Company Access

- VGC reserves the right to remotely access, monitor, and wipe company data from the mobile device in the event of a security breach, loss, or theft.
- VGC will not access personal data without the user's permission, except in circumstances where company data is at risk.
- You may be required at time to share client or candidate messages held on your device with VGC

Apps and Data Management

- Staff must only use approved apps for work-related activities.
- Confidential company or personal data should never be stored directly on the device but instead within designated company apps.

Connectivity and Charges

- All costs incurred on the personal device including voice calls, text messages, data usage, maintenance, and replacement are the responsibility of the device owner unless otherwise stated by the company.
- If the company provides a monetary allowance for device usage, guidelines will be issued separately.

Support

- The IT department will provide limited support for connectivity and access issues related to company resources and apps.
- IT will not provide support for device hardware, personal software, or non-approved apps.

Compliance

- Devices that are found to be non-compliant with this policy may be denied access to company resources and any monetary contributions will cease.
- Non-compliance with any part of this policy may result in disciplinary action.
- As well as monitoring devices remotely, VGC may use tools such as vulnerability scanners, penetration testers, and compliance checkers to assess the security posture and compliance level of the devices.
- VGC may also perform manual checks and interviews with employees to validate their adherence to this policy and the guidance as set by the Information Commissioners Office.

This policy will be reviewed annually, but updates may occur as technology and business needs evolve.

Signed **Dated:** 3 March 2025

Ciara Pryce
Chief Executive Officer

This policy confirms the commitments of all members of the VGC Group including VGC Labour Solutions, VGC Projects, VGC Personnel and Cole Hire.

Related Information