Policy and procedure

Approved: , Executive Director

Subject: Smartphone Access Policy

Effective date: Dec. 1, 2022

Questions: Tim Feld, Information Technology Manager

Purpose

DRCOG employees routinely request access to their DRCOG email using their personal smartphones. Although we recognize this desire, Information Technology cannot fully support such devices. However, arrangements can be made for access to DRCOG email provided employees agree and adhere to this policy.

This policy defines the level of Information Technology support offered to employees with personally owned smartphones as well as DRCOG-owned smartphones. This policy also describes the responsibilities of those granted smartphone access.

This policy also addresses smartphones used in a HIPAA-compliant environment.

Procedure

Requirements

Information Technology

Personally owned smartphones: Information Technology will provide the smartphone configuration settings needed to connect to DRCOG email. Additional support needs are to be handled by the employee through their cellphone provider.

DRCOG-owned smartphones: Information Technology will provide complete support.

Employee

Personally owned smartphones: The employee will use the information provided by Information Technology to configure the smartphone.

The employee will enable and maintain password security on the smartphone. The employee will not disclose the password to anyone.

In the event of technical problems, Information Technology will verify the accuracy of the information provided and the account configuration settings on the DRCOG Exchange server. If necessary, the employee will then seek further technical support from their cellphone provider.

The employee will complete the *DRCOG Smartphone Access Acknowledgement of Receipt* form and return it to Information Technology prior to being granted access.

DRCOG-owned smartphones: The employee will enable and maintain password security on the smartphone. The employee will not disclose the password to anyone.

In the event of technical problems, the employee will seek assistance from Information Technology via the Ivanti help desk application.

The employee will complete the *DRCOG Smartphone Access Acknowledgement of Receipt* form and return it to Information Technology prior to being granted access.

HIPAA-compliant environment

DRCOG has standardized on Apple iPhones for employees who are subject to Health Insurance Portability and Accountability Act regulations. These iPhones are subject to additional policies and rules.

DRCOG-owned iPhones can be used for:

- Making and receiving phone calls.
- Sending and receiving DRCOG email.
- DRCOG-related internet browsing.
- Using DRCOG-provided web-based applications.
- Video conferencing.
- Text messaging.
- Scanning.
- Taking and storing photos.

Additional uses beyond those listed above must first be approved by the HIPAA Compliance Coordinator.

Usage policy

- Only DRCOG-owned iPhones may be used.
- Use of personal cellphones is not allowed.
- Text messaging is allowed only if using a DRCOG-approved secure text messaging app.
- E-mail used to send protected health information data must be encrypted per the DRCOG-approved procedure
- The iPhone's operating system (iOS) must be kept updated.
- The iPhone must not be used on an unsecure wireless network.
- The iPhone must not be used on a public wireless network (such as one provided by a coffee shop, restaurant or airport)
- Cloud-based file sharing apps may not be used (for example, iCloud, Dropbox, OneDrive or Google Drive)
- Documents may be scanned only if using a DRCOG-approved and configured scanning app.
- Lost or stolen iPhones must be reported to DRCOG management immediately.

iPhone security settings

The iPhone security settings are applied by Information Technology personnel at the time of deployment. The user must not change these settings.

Responsibilities

Employee

Personally owned smartphones: If the smartphone is no longer used for DRCOG-related business purposes or the employee ceases to be employed by DRCOG, the employee will erase all DRCOG-related data from the smartphone.

If the smartphone is lost or stolen, the employee must immediately report the event to management and to Information Technology. The employee must also immediately report the event to their cellphone provider.

It is the employee's responsibility to take all prudent and preventative measures in safeguarding confidential DRCOG information accessed via the smartphone. The employee will immediately report any incident or suspected incident of unauthorized access or disclosure of confidential DRCOG information to Human Resources and to Information Technology.

The employee agrees to complete the *Smartphone Access Acknowledgement of Receipt* form and return it to Information Technology prior to being granted access.

DRCOG smartphones: If the employee ceases to be employed by DRCOG, the employee will return the smartphone to Human Resources. If the DRCOG smartphone is lost or stolen, the employee must report the loss to DRCOG management immediately.

DRCOG

DRCOG is not responsible for damages to or loss of data resulting from the use of a personal smartphone to access DRCOG email.

DRCOG reserves the right at any time to suspend the employee's access and require the DRCOG email account be removed from the smartphone.

Compliance

DRCOG does not permit a nonexempt employee to work outside of their normally scheduled work hours without the approval of their supervisor. Therefore, nonexempt employees are expected to refrain from reading and responding to business related email outside their normally scheduled work hours.

The employee agrees to adhere to this procedure as well as all relevant computer usage policies and document security policies implemented at DRCOG.

Failure to comply with the *Smartphone Access Policy* and/or all relevant computer usage policies and document security policies implemented at DRCOG may result in the disabling of DRCOG email smartphone access.