Introduction

Purpose of Policy
To establish the scope and process governing support of Mobile Devices used by SoD Faculty, Staff and Students.

Audience
All UNC SoD Faculty, Staff, Students, Visitors and Temporary Employees requesting OCIS assistance in troubleshooting and/or configuring Smartphones, Tablets or other mobile computing devices.

Definitions
Mobile Computing Device¹ – A mobile computing device² is a type of computer that can be easily transported and uses batteries to operate, so the device can be used from anywhere, and uses a special mobile operating system. A mobile computing device allows a user to work from any location and access the Internet through a cellular network or at a Wi-Fi hotspot. Mobile devices are smaller and more lightweight than traditional computers while still carrying the same functionality. A laptop computer running a standard operating system is not covered by this definition or policy.

OCIS – The SoD’s Office of Computing and Information Systems.

P2P – Peer-to-Peer file sharing (P2P) allows users to download media files such as music, movies and games using a P2P software client that searches for other connected devices. The “peers” are computer systems connected to each other through the Internet.

Smartphone – A cellular phone that is able to perform many of the functions of a computer, typically having a relatively large screen and an operating system capable of running general-purpose applications³.

SoD – UNC School of Dentistry

UNC email – The University’s electronic mail system. UNC email is considered by the school as sensitive because of the transmission and receipt of HIPAA-related information between faculty, staff, students and external health care providers.

Tablet – A tablet computer, or simply tablet, is a mobile computer with display, circuitry and battery in a single unit. Tablets come equipped with sensors, including cameras, a microphone, an

¹ Downloaded from: http://www.ehow.com/list_5951440_types-mobile-computer-devices.html November 17, 2014
² In this context, ‘computing device’ means a tablet or smartphone.
³ Downloaded from: http://www.oxforddictionaries.com/us/definition/americang_english/smartphone
accelerometer and a touchscreen, with finger or stylus gestures substituting for the use of computer mouse and keyboard⁴.

**UNC-ISO** – The University Information Security Office. The University’s Information Security Office oversees the security of the University’s electronic information.

**Policy**

**Policy Statement**
Tablets and smartphones are subject to the [SoD Bring Your Own Device (BYOD) Policy](http://www.bing.com/search?q=tablet+definition&qs=SS&pq=tablet+definition&sc=2-17&sp=1&ccid=5e1d6d497f214dc4b30fd82976a98385&FORM=QBRE). Faculty, Staff and Students must:

1. Submit the device and request permission for its use;
2. Permit OCIS technicians to examine the device to ensure it meets University and School security requirements;

OCIS support for tablets and smartphones is limited to the following:

1. Assistance in connecting the device to the UNC and SoD email and calendar systems as approved by OCIS;
2. Assistance in encrypting the device;
3. It is the owner’s responsibility to contact the device vendor in the event of additional support needs.

**OCIS reserves the right to determine the level of effort and support provided on a case by case basis**

**Compliance**

**Compliance Statement**
Failure to adhere to this policy, its procedures and standards may affect the ability of OCIS to provide prompt technical support to the school’s Faculty, Staff and Students. People and programs that fail to adhere to this policy, its procedures and standards may lose access to SoD systems, servers or services from the mobile device.

**Roles and Responsibilities**
OCIS –

---
⁴ Downloaded from: http://www.bing.com/search?q=tablet+definition&qs=SS&pq=tablet+definition&sc=2-17&sp=1&cvid=5e1d6d497f214dc4b30fd82976a98385&FORM=QBRE
School of Dentistry Office of Computing and Information Systems
Mobile Device Support Policy

1. Confirm the Mobile Computing Device meets SoD requirements
2. Conduct “good faith effort” to assist SoD Faculty, Staff and Students to properly configure\(^5\) personally owned Smartphones or Tablets.

Faculty, Staff & Students –

1. Deliver the Mobile Computing Device to the OCIS Office (Rm 0113 First Dental Building)

**Procedures to comply with policy**

Users seeking to connect Mobile Computing Devices to the SoD network must be submit such devices to OCIS to determine if and how the device can safely access SoD system, servers or services. OCIS personnel will make necessary recommendations to ensure the device meets University policy to access University and SoD resources.

**Standards to comply with policy**

1. Smartphones and tablets that directly access SoD e-mail are required to enable the device’s onboard device encryption, failed password attempt lockout, required password and remote device wipe capabilities.
2. Smartphones and tablets are prohibited from saving any confidential University or Sensitive Information\(^6\) on a smartphone or tablet computer.
3. Smartphones and tablet users are responsible for ensuring their device meets minimum campus computer security requirements for recommended antivirus software\(^7\) and required software security.
4. Smartphones and tablets are prohibited from running P2P file sharing applications on the SoD network. The existence of these programs on a smartphone or tablet computer places the user in violation of this policy.
5. Smartphone and tablet computer users are responsible for ensuring their device has the proper version of local applications installed to access SoD systems, servers or services.
6. OCIS and the UNC-ISO reserve the right to monitor a smartphone or tablet computer’s access\(^8\) to university e-mail and perform a remote wipe of the device and/or installed storage cards if University data or sensitive information is at risk.

---

\(^5\) Used in this context, ‘configure’ means enabling the device’s onboard encryption, failed password attempt lockout, required password and remote wipe capabilities

\(^6\) See UNC-CH School of Dentistry Secure Data Policy

\(^7\) See UNC-ITS Help and Support Page for recommended products

\(^8\) This statement does not imply actual reading of personal e-mail
School of Dentistry Office of Computing and Information Systems
Mobile Device Support Policy

Related Data

Appendices

Regulations

Statutes

Policies
1. UNC-Chapel Hill Campus Standards for Electronic Media Disposal
2. University of North Carolina Network Acceptable Use Policy
3. E-Mail Address Policy
4. Incident Management Policy
5. Information Security Policy
6. Institutional Data Governance Policy
7. Password Policy for General Users
8. Transmission of Protected Health Information and Personal Identifying Information Policy
9. Vulnerability Management Policy

Contacts

Questions
David B. Rankin, IT Director SoD, Security Liaison SoD 919-537-3485

Violations
David B. Rankin, IT Director SoD, Security Liaison SoD 919-537-3485

Consulting
OCIS Staff, 919-537-3485
UNC Help Desk, 919-962-4357
UNC Information Security Office, 919-445-9393

History

<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TBD</td>
<td>TAD</td>
</tr>
</tbody>
</table>

Next Review Date

Effective Date:
School of Dentistry Office of Computing and Information Systems
Mobile Device Support Policy

Authorization

David B. Rankin, Director Office of Computing and Information Services, UNC School of Dentistry

Signature ______________________________________________

Date _____________________________________________________