Solano County
Office of Education

Lisette Estrella-Henderson, Superintendent of Schools
5100 Business Center Drive, Fairfield, CA 94534-1658
707.399.4400 ★ www.solanocoe.net

PODD Agreement - Personally Owned Data Devices

Employees may request to have their SCOE email, calendar and other data synchronized with a personally-owned data device (PODD). Requests must be submitted in a technical support ticket stating the type of device (iPad, Android phone, iPhone, etc.) and the name of the supervising manager (per below). Employees must certify that they have read this agreement, and the supervising manager must approve the request within the technical support ticket.

This document is intended to provide overall guidance on the storage of SCOE-owned business data on personally-owned-data-devices (PODD). It is not intended to cover every possible situation or every possible technology. A Personally-Owned Data Device (PODD) is a device that stores, sends, receives or processes digital data, including mobile phones, notebook or desktop computers, digital, flash memory, and removable media (eg., magnetic or optical disks) or similar storage devices, which is not owned by the Solano County Office of Education.

SCOE-owned business data includes digital information that are stored or created by or for the Solano County Office of Education in the course of its operations, including any and all electronic messages, contacts, calendar entries and related data stored on SCOE's messaging servers. It includes all data files created, sent or received for business purposes. While all messages and data sent across any part of SCOE's network are subject to SCOE's acceptable use policies, including inspection and recording and retention by authorized managers, some data is not considered SCOE-owned business data. For example, data that is transmitted without being saved or retained on SCOE equipment, and which is not used in the conduct of SCOE's official business, is not generally considered SCOE-owned business data for the purposes of this policy. An example of this type of non-business data might be a personal message or file attachment that an employee downloads from their personal e-mail account to a personal flash drive through an open or publicly-available network connection provided by SCOE. Use of the SCOE network for non-business purposes is addressed by SCOE's Acceptable Use Agreement.

Storage of SCOE-owned business data on any PODD is strictly prohibited unless that privilege is specifically granted to an employee, and approved by the departmental manager at or above the level of Director. Authorization is valid only for a specific period of time, and only upon the employee reading and agreeing in writing to the terms of this privilege.

Key elements of this agreement:

- Any PODD that synchronizes with SCOE messaging systems must be configured and maintained with a passcode, PIN or similar security option that restricts the device's use by unauthorized persons. If the device supports remote data erasure in the event of loss or theft, that service must be enabled and configured.

- Permission to keep SCOE-owned business data on a PODD may be revoked by SCOE management at any time for any reason.

- Any synchronization between a PODD and a SCOE data source must be initially enabled by the SCOE I.T. department after it receives authorization from the manager.

- SCOE I.T. staff are not expected or permitted to spend technical work time assisting staff in the general operation of their PODD. The I.T. department does not guarantee or offer after-hours support for any PODD

- Employees understand that confidential information should never be stored on any PODD unless the user is specifically authorized to store such data, AND unless it is stored in a suitably secured fashion.

- Any loss of a PODD that may contain SCOE-owned business data must be reported to the employee's manager as well as the SCOE I.T. department within 24 hours.

I acknowledge that I have read, understand, and will abide by the regulations of SCOE Administrative Policies 4040 and #3513.1 in its entirety and the technology security guidelines as noted above.

Name

date