INTRODUCTION

All persons who interact with Kare Bears – whether Board members, volunteers, area leaders, transportation drivers and indeed any residents using services – must be entered into the PEOPLE file of SchedulesPlus. This document will discuss how various authorities are assigned to those persons, as appropriate.

FUNCTIONAL AREAS OF THE SYSTEM

There are four distinct functional components to SchedulesPlus for Kare Bears:

ADMIN: the main system, where trained "administrators" can be authorized to perform the "customer-facing" aspects of the system: loan equipment, establish ride requests, register attendees at events; or be authorized to define and manage events, or perform various "setup" activities of the system itself.

DRIVER MODULE: a separate method of access for transportation drivers to have limited access to view and manage rides created in ADMIN

GROUP LEADER MODULE: a separate method of access for persons identified as a "leader" of a specific defined GROUP of volunteers to manage members of the GROUP.

PORTAL: a separate method of access for all persons in PebbleCreek to access very limited capabilities, such as registering for events, expressing interest in being a volunteer; or for trained volunteers, to sign up for specific roles. *Note that SchedulesPlus calls this "Home USE" internally. We prefer to call it "Portal"*

Yes, a person could interact with Kare Bears in all four components, but they would do so from separate Log In sites.

LOG IN SCREENS and WEB ADDRESSES

A person will have only one password assigned, functional for all of these accesses, along with their email address.

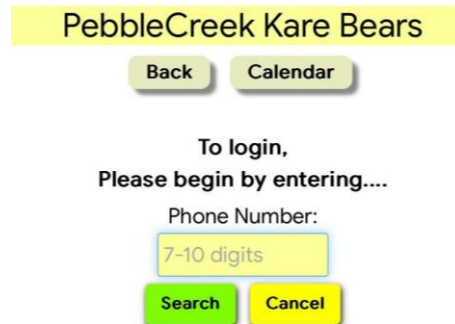| Log in for ADMIN	Log In for Driver Module	Log In for Group Leader
schedulesplus.com	shedulesplus.com/ karebears/ driver	shedulesplus.com/ karebears/ group

The Portal does not require a password, only the user's phone number

Initial Display – Portal	After the Log on button - Portal
schedulesplus.com/karebears	

HOW ARE AUTHORIZATIONS SET FOR THOSE AREAS

PORTAL: Kare Bears will (after the testing period) allow any user to access the Portal. If the person is not currently in our file, they will be able to add themselves – requiring First Name, Last Name, Full Address, Phone and Email.

Once entered into the file (previously or by that process), a person can access the pre-defined limited capabilities of the Portal (see separate documentation). This is the only access they have to the system in any manner.

DRIVER MODULE: Once established as a Driver for Kare Bears, the person will be assigned a temporary password (if not previously established) to use with their email address, to be able to sign in the Driver Module.

From the module, the Driver can: manage their password, view rides, signup (accept) rides currently unassigned to any driver, and report the completion of their assigned rides, with appropriate mileage totals. (see separate documentation).

GROUP LEADER MODULE Once established as a Leader for specific Group for Kare Bears, the person will be assigned a temporary password (if not previously established) to use with their email address, to be able to sign in the Group Leader Module.

From the module, the Leader can: manage their password, view the list of group members, add or delete members to/from the group, send email to all or selected members of the group. (see separate documentation).

ADMIN: Appropriate persons will be authorized as "administrators" in the ADMIN system by an invitation, sent with a temporary password (if not previously established). Upon their first log in, or at any other time, the person may change their password.

An administrator will be assigned one of three basic levels of authority:

- READER: can only READ information presented to them. No EDIT authority
- EDITOR: can read all information presented, to them, and can EDIT information, with some limitations, such as with respect to deletions.
- MANAGER: can read and edit all information presented to them, including the capability to delete.

The next sections will discuss how the system determines what information is presented to an individual administrator.

GENERAL DISCUSSION OF THE TAB METHOD OF SYSTEM PRESENTATION

The ADMIN screen presentation for each administrator will display (initially) two rows of tabs for various functions. Selecting a first-row tab will typically expand the selection of tabs on the second row, to provide access to detailed parts of that main function. A third row is possible, typically further expanding second-row functions.

Authorizations to specific functions are established by allowing or dis-allowing the presentation of various tabs to the individual administrator. Each administrator is set to a set of tabs that they will see, customized to the functions they are authorized to perform. These settings are assigned by the System Administrator(s) - currently Mark and Cary.

For example, we have a very limited presentation defined now for administrators who are only authorized to see the Office shift schedule. This is in use now for initial training of Office Volunteers. Here is what is presented:

Home
Schedule List	Volunteering

YOUR AUTHORITY LEVEL: READER   Your account owner and c
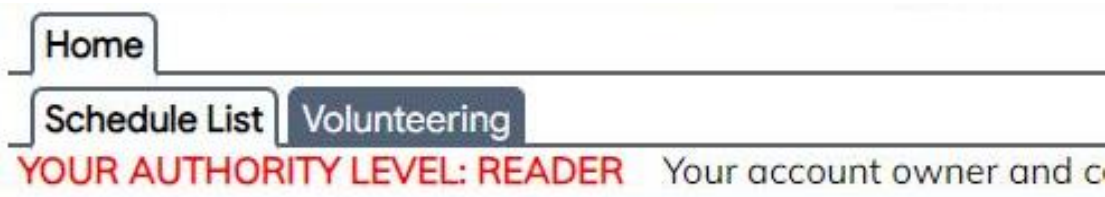
Once we are "live" fully using the system, this is a DRAFT of the presentation for all Office Volunteers (subject to final determination!)

Home	People	Calendar	POS	Rides
Schedule List	Volunteering	Actions

YOUR AUTHORITY LEVEL: EDITOR

Note: "POS" is short for "Point of Sale". The process of loaning equipment is here.

Note also that there are additional areas below the displayed tabs, most of which can be ignored by Office Volunteers. That will be explained in further training sessions. But the *basic functions are accessed through the tabs* *presented.*

Detailed instructions on the USE of each tab are discussed in the appropriate PROCEDURE documents - not described here.

==

These next functions are reserved to System Administrators, but they are summarized here to provide explanation of the overall scheme.

==

ASSIGNING 1) BASIC AUTHORITY LEVEL 2) MODULE ACCESS 3)PASSWORD

Begin at the PEOPLE record for the person. Click the ADMIN UPDATE button

These three updates may be made separately as each is needed

1) Then on the next screen, set or change the basic level to READER, EDITOR or MANAGER. Use NONE if you are <u>only</u> giving authority to one or more of the Modules – thus no access to ADMIN.

2) Select YES for either of the Modules where the person should be authorized. (We are not using the "Provider" Module)
3) You can force update the user's Password with the option shown at any time. (Useful if they forgot their password)

Click the SAVE button lower on the page (not shown) to complete any of these three ADMIN UPDATE types.

<u>An email is sent to the user for any of these initial settings or updates!</u>

CREATING AUTHORIZATIONS AND ASSIGNING TO ADMINISTRATORS

Authorizations to specific functions are established by allowing or dis-allowing the presentation of various tabs to the individual administrator. To make assignments, first select an administrator from the drop-down list (Sue Pelletier shown).

To define the presentation to the administrator, system, there are numerous settings here which cause specific tab(s) to become visible to the user (box is blank) or to be hidden from the user (box is red). There are such settings in each of the major functional areas listed at the left. This example shows the settings for RIDES.

Note: We may not be using some of those major functions – Services or TRP for example – but they are shown included at the left for possible settings

Access the ACCOUNT tab, then the SECURITY tab, then the HIDE TABS tab

As can be imagined, there are thus over 100+ settings for each administrator. Later in this document we will see how the system can establish a ROLE – a named definition of all 100+ settings - which can then be applied *in bulk* to an administrator, rather than discretely making each setting in each major area.

For the moment, let's continue with checking or un-checking individual boxes.

If you make a change to any box setting, click the SAVE FOR THIS ADMIN button – which saves <u>all</u> box settings in <u>all</u> of the major functions (at the left) which you have set or changed in the current session for this administrator. To back out before saving, the RESET button will revert to all the person's settings as they were before this session started. *Please avoid the UNHIDE ALL button, which would give the user access to everything!*

You must click the SAVE FOR THIS ADMIN button to apply your changes.

Note: If the administrator is logged in during this update, they must log out, then log in again for the changes to be reflected.

CREATING ROLES - AND ASSIGNING TO ADMINISTRATORS

The right-hand side of the same screen discussed above is now shown here

Some administrators will have very customized settings tailored to their particular responsibilities – perhaps unique.

However, for instance, we will want to assign the same capabilities to all Office Volunteers.

The concept of ROLE allows for creation of a named set of <u>all</u> box settings in <u>all</u> major areas. The named ROLE can then be "preloaded" for a given administrator, rather than making the 100+ individual settings.

To grant such a standard set of authorizations to a particular administrator, bring up that in-process person on the ACCOUNT-SECURITY-HIDE TABS screen. Select an <u>already defined</u> ROLE from the drop-down box named PRE-LOAD THIS ROLE.

Upon making that selection, an on-screen message will confirm that selection, and prompt to click the SAVE FOR THIS ADMIN button. Upon that click, all the settings will then refresh, now assigned to the person.

Note: We could be assigning authorities to the "in-process" person for the first time, or revising authorities for that person with previous authorities

A ROLE is newly created by using the manually established settings for one particular administrator. Rather than using any real persons, we have created a few "phantom" users, solely as place-holders for these definitions. Currently there are:

Phantom person	Named ROLE
Default Schedule	TRAINING 1
Default Office	OFFICE
Default Admin	ADMIN

The numerous individual 100+ settings will have previously been made on the record for each of these phantom persons, and saved by clicking the SAVE FOR THIS ADMIN button.

Those settings were then established as a named ROLE by:

1. entering the intended ROLE name in the SAVE AS NEW ROLE box
2. click SAVE ROLE.
3. That ROLE is now available to PRE-LOAD to ana administrator

The definitions of a ROLE cannot be edited. The ROLE must be deleted and recreated – after appropriate changes are made to the desired new settings.

A) Select the phantom person for whom authorities are to be modified
B) Modify settings in any major area(s) (left groupings) as now needed.
C) Click SAVE FOR THIS ADMIN. A message will confirm.
D) Select the ROLE name to change (delete and recreate) in the DELETE A ROLE box
E) Click DELETE. A message will confirm.
F) SAVE AS NEW ROLE per steps 1) and 2) above, using the same name

Note: Deleting a ROLE does NOT affect any settings that had been made to any administrators previously by applying that ROLE to them, as it existed at the time.