



**North Carolina Reading First**

**Department of Public Instruction  
Personal Data Assistant  
Acceptable Use Policy  
June, 2004**



Personal Data Assistant  
Acceptable Use Policy

## Table of Contents

<u>Introduction</u> .....	3
<u>Security</u> .....	3
<u>Risks</u> .....	3
<u>Calendars, et al</u> .....	3
<u>Theft/Loss</u> .....	4
<u>Personal Device Ownership</u> .....	4
<u>Malicious Software</u> .....	4
<u>Licenses</u> .....	5
<u>E-mail</u> .....	5
<u>TPRI</u> .....	5
<u>Attachment</u> .....	7
<u>Signature Sheet</u> .....	7



Personal Data Assistant  
Acceptable Use Policy

## Introduction

As a user of Wireless Generation's TPRI, you know today's mobile devices offer many benefits to the education community. By converting the TPRI paper-based assessment to a form-based assessment such as that offered by Wireless Generation, Personal Digital Assistants (PDA) improve productivity, reduce operational costs and provide a better educational experience for students.

Along with these great improvements come security concerns over lost or stolen data. Please review the following acceptable use policy, sign and return to your instructor. If you have questions about this policy please contact Sara Thomas at [sathomas@dpi.state.nc.us](mailto:sathomas@dpi.state.nc.us) or Steve McCutchen at [smcutch@dpi.state.nc.us](mailto:smcutch@dpi.state.nc.us).

## Security

To provide the highest level of security, PDAs must be secured at three points:

- ❖ **Access to the device.** Because the small size of the PDA makes them susceptible to being lost or stolen, devices need to be able to verify that the person attempting to access them is a legitimate user. This is done via a password.
- ❖ **Access to stored data.** The storage cards that fit into mobile devices' expansion slots can store anything from a small amount of data to five gigabytes or more. Removable storage heightens the concern about data falling into the wrong hands. Because of this concern, applications associated with Reading First will not use removable storage and PDA users should not purchase them.
- ❖ **Access to networks.** Connectivity provides access to sensitive student data stored on the Web. Security is needed at this point to prevent unauthorized access to information stored on these networks.

## Risks

### *Calendars, et al*

The calendar is an integral part of the PDA. It is convenient to use. It is worth considering what would happen if your calendar fell into the hands of a student or became public knowledge. It could at least be embarrassing. If you recorded social security numbers or identification numbers, it could be a violation of the law as defined by the Family Educational Rights and Privacy Act



Personal Data Assistant  
Acceptable Use Policy

(FERPA). Therefore, access to the device should be restricted by a password of at least four characters. The password should be changed regularly; at least every ninety days. Individual identification numbers or other sensitive information should not be entered in any of the applications that reside solely on the PDA including:

- ❖ calendar;
- ❖ contact;
- ❖ note pad;
- ❖ documents; and
- ❖ memos.

## *Theft/Loss*

Industry estimates indicate that hundreds of thousands of cell phones and handheld devices are stolen or lost each year. The problem with a stolen or lost device is twofold. First, the teacher does not have the device to use until a new device can be supplied and set up. Second, the data stored on the device may be of value to others and may compromise privacy. Such losses reinforce the policy of maintaining a valid password on the device and not entering personal identifiers in applications residing solely on the PDA.

## *Personal Device Ownership*

Personal ownership of mobile devices and add-ons moves control away from the organization. When data belonging to the school resides on a device owned personally by an employee, a clear conflict of interest can arise—one that can have adverse effects on data security. For this reason, no personal PDAs or add-ons should be acquired for Reading First.

## *Malicious Software*

Although mobile-based devices have yet to become a significant target for malicious code, one may argue that it is only a matter of time before such threats occur. Also, even if the devices themselves are not affected by such code, when they connect to the network they can serve as transport mechanisms for passing destructive software on to other computing systems. Malicious software can take a number of forms, including viruses, Trojan horses, and worms. Viruses are usually propagated through some kind of user-initiated action, such as opening an attachment or running a script or application. They attempt to spread undetected through the system by attaching themselves to other files. Trojan horses are programs that masquerade as genuine applications in order to perform some unauthorized



Personal Data Assistant  
Acceptable Use Policy

activity once they gain access to a user's system. Worms destroy data as they work their way through a system.

Unauthorized software should not be loaded to the PDA. The origination of emails should be reviewed and those that look suspicious or if the sender is not recognized should not be opened. The PDA has the facility to communicate with other PDAs using the infrared port. This facility presents an opportunity to transmit viruses; this capability should not be used with strangers.

## *Licenses*

The policy of the State of North Carolina is that all employees and contractors must follow applicable software copyright and licensing laws.

## *E-mail*

Electronic mail or E-mail is not a secure medium. Therefore, social security numbers and other identifiers should not be transmitted using email. When sending or forwarding E-mail, users shall identify themselves clearly and accurately. Anonymous postings are forbidden.

## *TPRI*

The Reading First application as implemented by Wireless Generation's TPRI requires a password in addition to the one for the device. They should not be the same passwords. Passwords should be maintained in a secure manner. Do not tape them on devices, or leave them where they are available to others.

From time to time, reports will be printed with student information. These should not be left unattended. When reports are to be discarded, they should be shredded.

TPRI uses a desktop computer as a Sync station. This synchronization system performs two principal functions:

1. It reconciles data between the Web server and your PDA. This allows minimal data to be housed on the PDA; only the student name is maintained on the device.
2. It automatically and transparently updates application and data file on the PDA when Wireless Generation releases updates to the software.

The Web server houses all TPRI data in an approved secure manner. In the case of inadvertent data corruption or loss on the PDA, the Wireless Generation data exchange application is able to restore the state of the TPRI application



Personal Data Assistant  
Acceptable Use Policy

on the PDA to an earlier, stable state. Since the Web is an integral part of the TPRI application, security issues abound relating to the Internet. Therefore, the policy relating to the use of the Internet is attached to this Acceptable Use Policy.



Personal Data Assistant  
Acceptable Use Policy

# Attachment

## *Signature Sheet*

District:

---

School:

---

Name (Last, First):

---

I have read, and understand the document titled, "Department of Public Instruction, Acceptable Use Policy" dated June 2004, and agree to abide this DPI policy and all statewide data security related policies.

---

Signature

Date