Introduction

This document contains the release notes for RMU Version 3.1. Three new functions are provided in this release of RMU:-

1. Freezing/Unfreezing of devices via RMU
2. Fleet-Check (aka Stock-Take)
3. Devices not handed-in at the end of the day by students who have signed partial charters

Freeze/Unfreeze of Devices via RMU

RMU will provide the means to initiate the freezing/unfreezing of devices. Freeze actions can happen in one of two ways. Either a TSO has been given instructions from the principal to freeze a device (according to policy), or RMU automatically freezes a device if it is reported as lost or stolen.

A request to freeze/unfreeze a device (either automatically or manually) will trigger an email to be sent to the principal. The email informs the principal of the freeze action which is about to occur and gives the principal some time to place a halt on the action if he/she wishes.

A few days after the freeze action has been triggered it will be processed on Computrace. The processing of the freeze actions on Computrace will be a manual (undertaken by the Information Security Unit).

Freeze actions are non-destructive. However, it is essential that freezes are not misused (i.e. the TSO must not freeze a student’s device to “punish” him/her). A region-wise dashboard of bulk freeze activity is provided to enable the regional manager to monitor the manually triggered bulk freeze activity in his region.

Manually Triggered Bulk Freeze/Unfreeze of Devices

The principal will advise the TSO to enact the freeze/unfreeze of a device. The TSO identifies the devices to be frozen/unfrozen, and initiate the freeze/unfreeze action. The screen image below shows how the freeze/unfreeze is done.
When the TSO initiates the freeze, a pop-up (shown below) is displayed prompting the TSO to enter a “freeze reason”, e.g. “Student refuses to bring device to school despite numerous requests to comply.” It is not permitted to leave the “freeze reason” blank.

The display of candidate devices for the freeze action has logic whereby if a device is already frozen, or there is a pending freeze request against it (due to the device being marked as lost or stolen in the past few days but the freeze not having yet been actioned - see later), the device will not be allowed to be manually frozen. Similarly, you cannot manually unfreeze a device if it has a pending unfreeze already active for it, or the device is not frozen.
RMU will pop-up a warning if the TSO attempts to unfreeze a device that is currently lost/stolen.

Freeze/unfreeze will not be available for devices in the DET pool (reason: the development effort to provide this functionality is not deemed to justify the benefit). On the rare occasion that a device in the DET pool has to be frozen/unfrozen, this request will be conveyed directly to the Information Security Unit for processing.

Automatically Triggered Freeze/Unfreeze of Devices

RMU will initiate an automatic freeze/unfreeze action on a device if the device is lost, stolen, found or recovered. Losses and thefts will cause a device to be frozen; finds and recoveries will cause a device to be unfrozen.

Automatic freeze/unfreeze actions happen according to the following schedule:-

- Device reported as lost in RMU – placed on the list for freezing after 7 days
- Device reported as stolen in RMU – placed on the list for freezing after 2 days
- Device reported as found/recovered in RMU – immediately placed on the list for unfreezing

N.B. Information Security Unit will not action a freeze request until the appropriate “cooling-off” period has expired; and even then, it is unlikely that such request will be actioned straight-away. This gives a time-window so that the principal can halt a freeze (or unfreeze) action for lost or stolen devices.

Email to Principal Advising of Freeze/Unfreeze

Once the TSO has triggered the freeze/unfreeze action (either automatic or manual), RMU will send an email to the principal giving notification of the freeze/unfreeze action which is about to occur. The principal does not have to do anything on receipt of the email unless he/she wishes to stop the action, in which case he/she has to contact the TSO in the first instance, or the Information Security Unit.

Principals receive the email in real-time as soon as the freeze/unfreeze action happens. A sample of the email follows:-
Freeze Message

Although Computrace can support a number of different “freeze messages”, for simplicity there will be only one generic freeze message (the so-called White Screen of Death):

```
This device has been frozen by the NSW Department of Education and Training. If you are a student/teacher, please contact your TSO to have the device unfrozen. If you have found this device, please return it to any NSW government school or a police station.
```

Withdrawing a Pending Freeze/Unfreeze Request

Freezes and unfreezes do not happen in real-time. There can be a few days delay between a freeze/unfreeze action being requested, and the action being processed. Occasionally there will be a need for the TSO to withdraw a pending freeze/unfreeze request. For example:

- A device might have a pending manual freeze request against it but the principal decides to halt the freeze because he/she has changed his/her mind in the light of new information to hand
A system generated unfreeze action is proposed because a lost device has apparently been found, but the principal decides to retain the freeze action on the device.

The TSO can use RMU to withdraw a pending freeze/unfreeze action. The withdrawal of pending freeze/unfreeze actions must be done on a device by device basis; there is no facility to perform a bulk withdrawal of freeze/unfreeze actions.

The screen image below shows the Compliance tab for the device:

The TSO checks the “Withdraw Compliance Request” button (only enabled if applicable for the device). On clicking the button, RMU will prompt “Are you sure that you wish to withdraw the pending freeze/unfreeze action?”.

An email is sent to the principal advising of a withdrawal of a freeze/unfreeze request. A sample of the email follows:

```
From: do_not_reply@det.nsw.edu.au [mailto:do_not_reply@det.nsw.edu.au]
Sent: Friday, 1 April 2011 2:41 PM
To: Frost, Warren
Subject: Notification of RMU Withdrawal Action

Attention The Principal,

Please be advised that the TSO has withdrawn the following action:

**Unfreeze Device**

L3 AVCOB  Not Assigned  Device has been reported as found in RMU

If you wish to query the action given above, please contact your TSO.

This email is automatically generated by RMU. Please do not reply to this email since the mailbox is not monitored.
```
Log of Freeze/Unfreeze Activity

Freezes/unfreezes do not happen in real-time – the freezes/unfreezes are processed on a regular bases by the Information Security Unit. RMU will provide the TSO with feedback on the freeze/unfreeze status of a device. The feedback is provided in the Compliance tab of the device, as illustrated in the screen image above. Entries in the log are displayed in chronological order, most recent at the top.

Freeze Dashboard

The Freeze Dashboard is intended to give regional managers the opportunity to “keep an eye” on the freeze/unfreeze activity in their region. The dashboard allows the regional manager to select a date range for monitoring, the default being the last four weeks. Each TSO’s activity is reported at each school where the TSO operates. The regional manager can sort the columns to assist with his monitoring.

The dashboard only shows where the TSO has undertaken a manual freeze/unfreeze action; automatic actions due to devices being lost/stolen are not reported.

Per-Device Unfreezing Using Pass-Code

Occasionally there will be a need to unfreeze a device using a pass-code, rather than wait for the processing of unfreezes to be processed via RMU. For example, a student’s device might have been incorrectly frozen, and there is a need to remediate the freeze to lessen student stress.

There are also technical reasons which will cause a bulk unfreeze not to work such as hardware issues, filtering policies, call success rates, etc.; in such cases a pass-code unfreeze may be required. RMU does not offer a-per device unfreeze using pass-code because the frequency of
such requests is not thought to be high enough to warrant automating a solution. Where a per-
device pass-code is required, the principal and/or TSO will need to contact the Information
Security Unit.

Fleet Check (aka Stock-Take)

A new menu ‘Fleet Check’ is on the main menu list in RMU. This menu loads a screen with three
tabs:

- Fleet Check Device
- Admin
- Reports

Depending on your access rights in RMU, you might not see the Admin tab.

The “Fleet Check Device” tab will be selected by default when the user clicks on the Fleet Check
main menu. This tab allows the current Fleet Check to be performed on a device, as well as
viewing any previously completed Fleet Checks.

The “Admin” tab allows the creation and management of Fleet Checks by Device Type and
Vintage, as well as the management of questions. Only authorised users will have access to this
tab.

The “Reports” tab is used to obtain Excel spreadsheet reports of Fleet Check activity.

Fleet Check Device Tab

This tab permits Fleet Checks to be performed on a device. Initially, the tab presents a search
dialog in order to select a particular device (only devices at the user’s default school can be Fleet
Checked).
Upon typing/scanning a device serial number and clicking the Go button, the current Fleet Check that matches the device model is displayed. If no current Fleet Check is applicable, a notification popup is displayed.

All Fleet Check questions fall under one of three categories:

- External Hardware
- Internal Hardware
- Software

Each category can be expanded or collapsed on the screen for ease of viewing.

Questions in each category are answered using radio buttons. A scroll bar is available to the right of each expanded category to allow scrolling when questions exceed the display capacity of the screen.

The TSO works through each category. The Save button enables the TSO to save a partially completed Fleet Check for a device. The Fleet Check can be marked as completed by ticking the “Completed?” checkbox before saving. The screen will auto-save every 10 minutes.
A text box is provided at the bottom of the page, for additional comments at the completion of the Fleet Check for each device.

Once a device has been Fleet Checked and the Save button is clicked, the user is returned to the search dialog where another device can be Fleet Checked.

**Admin tab**

*This section is not relevant if you are not an RMU administrator. This said, there is no harm in reading this section to get an understanding of how Fleet Check works.*

The Admin tab is where an RMU administrator sets-up the Fleet Checks, as well as managing the questions and answer options for each Fleet Check. Fleet Checks will be created based on Device Type and Vintage (i.e. 4333 A18 Vintage 09) although in practice only the vintage will be used.

There are a pool of questions and the administrator will attach selected questions to a Fleet Checks during the creation process. The user can add new questions, which will be saved to the pool and can be used for future Fleet Checks if required.

The administrator can also edit existing questions or alter the answer types for questions (i.e. change items in drop-lists) if required.

A screen image below shows how to set-up a Fleet Check. The administrator names the Fleet Check (Vintage 10 Term 1 2011), selects the devices to be checked (Vintage 10), and sets a date range for the Fleet Check (06/04/2011 to 07/04/2011).

RMU will do a check on other Fleet Checks and advise the administrator if there is a clash with another Fleet Checks. In the screen image below, the Vintage 10 check clashes with a check called “Enter Name Here0” because the dates overlap and there is a vintage overlap. It is up to the administrator to decide what to do with clashes; the impact of Fleet Checking a Vintage 10 device on the 06/04/2011 is non-deterministic.
Having created the Fleet Check, the administrator can add the questions that he/she wishes to be asked. In the screen image below, the pool of questions is on the left, and the questions to be asked are on the right.
The administrator can add and edit questions in the pool. But note that it is not possible to edit a question that has already been “answered” in a previous Fleet Check.

Adding or Editing Questions

This section is not relevant if you are not an RMU administrator. This said, there is no harm in reading this section to get an understanding of how Fleet Check works.

New questions can be included, or existing questions edited, by using the ‘Add’ and ‘Edit’ hyperlinks that appear above the All Questions box. Clicking Add launches the following pop-up.

The question textbox is limited to 300 characters. The user must select a category to drop the question into, and choose one of three answer types:

- Pass / Fail radio buttons
- Pass / Minor Wear / Fail radio buttons
- Custom radio buttons

If Custom is selected, the administrator must type each radio button option into the ‘Item List’ text box. A comma separates each option, and the system will check for consistency when Save is pressed.
Reports Tab

The “Reports” tab permits Fleet Check reports to be generated. The reports are created in Microsoft Excel spreadsheet format (XLS) and emailed to the user. Each spreadsheet consists of two worksheets. The first worksheet is a summary page, and the second a list of devices with answers to the Fleet Check questions.

Device Not Handed-in at End of Day

A student may have signed a partial charter (as opposed to full charter). Such students do not take the device home and the student is required to leave the device at school at the end of each day. There is a need to report on breaches of the partial charter.
The TSO records that a device has been handed-out to a student. At the end of the day, the TSO records that the device has been returned.

A report will be available showing compliance with the partial charter conditions between a “from” date and a “to” date.
<table>
<thead>
<tr>
<th>SNR</th>
<th>Name</th>
<th>Serial Number</th>
<th>Handled Out Date</th>
<th>Handled To Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>ST10025</td>
<td>06/04/2011 12:42:00 AM</td>
<td>06/04/2011 12:47:00 AM</td>
</tr>
</tbody>
</table>

1 Record Found