



eT4L Primary system update

A major update to all eT4L servers in primary schools, SSPs and EECs will commence rolling out from mid-November.

The **Configuration Manager (CM)** component on the server currently runs the 2007 version and this will be **upgraded to CM 2012** to bring it in line with the eT4L servers currently rolling out into High Schools. Together with the server upgrade, **all Windows devices** will need their CM Agent updated via a centralised task.

The main benefit of the upgrade to primary schools is that **any T4L Windows 8.1 Tablets will now be able to be "F12-built"** and integrated into the eT4L environment.

A pilot at 41 schools has ended. Another 40 schools will be upgraded during week 6. **All remaining schools will be staged** from late November with an aim to **complete during Term 1 2016**.

As each school is scheduled, **notification will be provided** together with support resources to allow the school to access the new features.



Improving ICT services

Since May, Information Technology Directorate (ITD) has been working with key school staff to implement a range of measures to monitor and improve customer experience of IT services. These initiatives have directly led to a substantial improvement in service quality, availability and performance. This in turn has led to a significant reduction in incident reports.

In addition to the caching appliance and OS update blocking outlined in our previous newsletter, ITD has undertaken a range of improvement measures including:

- *End to end analysis of critical services and targeted remediation activities, such as that completed for ERN*
- *Quality of Service protocols for improved traffic management*
- *Better monitoring capabilities using systems that provide pro-active monitoring of user experience measurements for applications, Internet use and traffic profiling*
- *Working with individual schools and local support teams to resolve sources of "top talkers" which negatively impact bandwidth availability for educational and corporate applications*
- *Assessment of options to enhance the user experience of satellite schools*
- *PAC file management improvements.*

ISSUE

08

NOV 2015

this issue

Protecting yourself online **P.2**

Innovative learning spaces **P.3**

ICT quick news **P.4**

Investigations of DoE Network performance issues have led to more active monitoring, decreases in bottlenecks, and overall improvements in network services.

ITD will continue to work with the PPA, SPC and directly with schools to ensure that progress continues on a range of initiatives to further extend the benefits already provided. The already improved focus on understanding user experience and on end-to-end service quality, allows staff to focus on their core daily activities with greater assurance of minimal disruption. With enhanced and reliable ICT services, we can continue to support innovative educational solutions and deliver positive outcomes for all students.



Personal data security

An important concept that all ICT users should understand – *the easier it is for you to access your data, the easier it is for someone else to access your data.*

In this age of mobile personal devices with saved passwords to easily access cloud-based storage, email and social media, losing your privacy is as easy as losing your phone or tablet.

Using different passwords for different services, regularly changing your passwords and signing out of services when not needed will help to protect your data.

Avoiding data loss

Too many people still make the mistake of only having one copy of their files, documents or photos. Keeping all of your personal files on a USB stick because it's portable and handy is great, until something goes wrong with the stick, or it gets misplaced. Similarly, having documents only in MS Office 365's OneDrive or Google Apps' Drive means relying on Internet access and the service always being reliable.

Personal backup copies of all of your important files is essential. The mantra – *"A file doesn't exist unless you have at least two copies of it in different locations"* will help to avoid data loss.

WHY PHISHING SCAMS KEEP WORKING



What is Phishing?

When internet fraudsters impersonate a business to trick you into giving out your personal information, it's called **phishing**. Don't respond to email, text, or pop-up messages that ask for your personal, social or financial information. Don't click on links within them either – **even if the message seems to be from an organisation you trust**. It isn't. Legitimate businesses don't ask you to send sensitive information through insecure channels.

Don't be the one who falls for a Phishing scam!

Spam and phishing emails have been a fact of life for many years now. So much so that over 80% of all emails addressed to NSW DoE email boxes are caught by our spam filters and deleted before they even get to you.

Most users hardly get any spam as a result. However, some targeted spam and phishing messages still manage to get through from time to time. That's why it's very important that **all staff become proficient at identifying phishing scams** and don't blindly click on links or open attachments. Here are some tips you can pass onto staff:

- *Be suspicious of any email that **does not address you in the message by your name.***
- *The message often says **something bad will happen if you don't respond** – it's a trap.*
- ***Typos and poor grammar are common.** Look out for them like you are marking student work.*
- *Any **click here** type links that seem to take you to a URL unrelated to the original message are bad – even if the site looks OK. **Pay close attention to the URL of the link.***
- *Phishing is not always about your banking. It's more often about wanting your account credentials for any site or service. **Don't give your credentials away easily.** Be vigilant while online.*

Follow these tips, be observant and **don't get hooked.**

Be a little suspicious. Most phishing attacks rely on simple social engineering. People are the weak link in security. It's easier to trick people than it is to hack computers.

Malware and Identity Theft

Malware is short for 'malicious software.' It includes viruses and other software that get installed on your computer, phone, or mobile device with or without your consent.

These programs can cause your device to crash, or perform less reliably. They can be used to monitor and control your online activity. It's common for malware to be delivered via phishing – an email or online post that beckons you to click a link or open an attachment so it can install in the background.

Criminals use malware to steal personal information, capture keystrokes, send spam from your computer, or take over control of your device. With direct access to much of your personal information, identity theft is easily achieved. Being aware and proactively protecting yourself from identity theft is much easier than cleaning up the pieces after having been exploited.

Innovative Learning Spaces at Eight Central School



Information Technology Directorate, Asset Management Directorate and the Futures Learning Unit are working together to deliver options for future-focused, flexible learning spaces into schools.

These new environments will include the innovative integration of new technologies and furniture to provide better opportunities for student/teacher collaboration. To assist with the planning and delivery of these new ICT-rich learning spaces, a new "school" is being developed within ITD's offices at Eveleigh. The new "Eight Central School" won't have students or staff, but has its own school network with eT4L server and WiFi access. Once set up, it will be available for visits by teachers and their students to test the new facilities in real classroom settings.

Engaging features:

- bright, flexible, practical and easy to move furniture with a variety of breakout zones
- computers on wheels with touch screens and desktop conferencing
- interactive projectors and large interactive panels
- an array of mobile and tablet devices
- 3D printers and robotics kits
- classroom mobile device management and tools for collaboration.



A team from the Futures Learning Unit will be based at the new school and will work closely with ITD on the development of these new and exciting learning spaces catering for students from K to 12.



We look forward to the ICT opportunities that the *Eight Central School* will bring and the enhancement that this initiative will deliver to teaching and learning in schools across New South Wales.

If your school is interested in visiting Eight Central School, please send an email to - futures_unit@det.nsw.edu.au

New Pedagogies in New Spaces at Campbelltown High

Campbelltown Performing Arts High School has transformed a number of learning spaces across the school to more effectively support the implementation of new and emerging pedagogies.

The school has produced a Class-Movie to share their journey to new pedagogies through the opportunities that new learning spaces offer. A similar journey is taking place at Macquarie Fields High School as well.



Click the play button above to watch this video

Goodbye TaLe!

Learning Systems has announced that TaLe and TaLe4Students will be decommissioned on 1 February 2016.



Teachers should use **Scootle** to discover new learning and teaching resources. Scootle provides Australian teachers with access to digital resources that are aligned to the Australian Curriculum.

TaLe users who use **Lists and Saved searches** may like to explore **Learning Paths** in Scootle (see **FAQ #12**). Learning Paths allow teachers to select resources to use with learning activities. These can then be shared with students using a student PIN.

Future DoE produced resources will be published to Scootle. **NSW DoE teachers access Scootle via the Staff Portal.**



TaLe closes 1 Feb 2016



Google Apps and Office 365 Privacy

The DoE has clear privacy procedures which are underpinned by the **Privacy and Personal Information Protection Act 1998 (NSW)** and the **Health Records and Information Privacy Act 2002 (NSW)**.

Microsoft and Google both have privacy policies that explain how they deal with data stored in their systems. As Google and Microsoft are public corporations, they are subject to the **Commonwealth Privacy Act 1988**.

Information Technology Directorate along with the vendors, has produced two Fact Sheets to **clarify each of their privacy statements** which can be shared with parents who may have concerns following news reports on the topic.

- [Google Privacy statement](#)
- [MS Privacy statement](#)

MS Office 2013

With the coming release of **Office 2016** for enterprises, plans to roll out MS Office 2013 in eT4L schools during term 4 are now on hold. A new plan to **upgrade directly to Office 2016** is being developed. Further details will be provided next term.

2,000 schools migrated to eT4L!

On 16 October, ITD reached the impressive milestone of 2,000 schools fully migrated to eT4L Services.

All primary schools have been running eT4L Services successfully for the past few years. ITD recently passed the halfway mark of all secondary schools completed as another great milestone.



Microsoft's new Education site

Microsoft has recently updated its [website aimed at school education](#) and providing teachers with free resources to help them with integrating ICTs into their classrooms.

The site offers quick tip videos, detailed courses and training as well as curriculum guides and lesson plans created by educators. Connections can also be made with other teachers through the Microsoft Educator Community. It's worth investigating the site to discover new ways to leverage the DoE Office 365 service with students and staff, and to keep up with what other schools are doing around the world with ICTs.

Using Facebook safely: Poster

Facebook might well be blocked at school for valid reasons, but it doesn't mean we can ignore that it exists nor that our students are prolific users of the world's largest social network.

Here's [a useful poster](#) you can print and hang in your classroom so that at least while they are at school and off Facebook, they can think about how they should be using social networking appropriately.

Set your Secret Questions and Answers in Staff Portal?

While you're updating your profile by following the steps in the article below, you should also consider setting or revising your secret questions and answers in Staff Portal.

To do this, just sign into portal and click **Change Password** at the top, then click the link on the right to **set up your secret questions and answers**. These will enable you to regain access to your account without the need to log a service desk call by simply using the "I've forgotten my password" option on the portal sign-on screen.

It's important that your answers are not easily guessable. If someone can guess your answers, they can reset your password and use your department login to access your email, ESS and other services. A handy guide explaining the Secret Q&As [is available here](#).

Update your profile in Portal

The option in the Staff Portal (*at the top-right*) to update your profile has been modified and now individual staff can **edit their own Global Address List (GAL) details**, including their work location and contact details. If the details in the email address list about you are not accurate, you can use this tool to easily and quickly update them.

