



## Information and Communication Technology Service [Share](#) |

Enabling people

Search

- Admin ▶
- About ICTS ▶
- Core SLA ▶
- Helpdesk ▶
- Desktop Support ▶
- Anti-Virus & Security ▶
- Identity & Access Management ▶
- Training ▶
- Email & Newsgroups ▶
- Phone & Fax ▶
- Networking ▶
- Admin Systems ▶
- Academic Computing ▶
- Classroom Support ▶
- Research Computing ▶
- Student Computing ▶
- Web Publishing ▶
- Technical Writing ▶
- About This Site ▶
- Contact Us ▶
- Utilities ▶
- Web-based services ▶
- ICTS Staff only ▶

[About](#) >> **ICTS Bits & Bytes Newsletter Vol2 Number9**

[ [Edit](#) | [Delete](#) ]



Volume 2 Number 9

### In this issue:

1. [Managing your UCT mailing lists effectively](#)
2. [Be cautious when using peer-to-peer sharing](#)
3. [Social networking and personal security settings](#)



### October 2011 dates to remember:

#### [Scheduled maintenance slot](#)

The next maintenance slot is set for **16 October 2011** from 09:00 to 17:00.

#### [Develop your own electronic newsletter](#)

Learn the basics in the half day [Electronic Newsletter Design workshop](#) on **1 November** (13:30 - 16:30).

#### [Using the Internet more effectively](#)

Attend the [Effective Web Search workshop](#) from **03-04 November** (13:30 - 16:30) and learn a few tips and tricks on how to make the most of your time online.

ICTS TechFest in November  
Check out the latest gadgets, notebooks, printers and software at the ICTS Technology Festival (TechFest) from **17-18 November**.

#### **UCT contributes HPC resources to SAGrid**

You might have heard about Grid computing, but do you know what it

### October is Cyber Security Awareness month

This month's newsletter talks about 3 ways to protect yourself and your information.

#### **Managing your UCT mailing lists effectively**

Emailing large groups of people is so much easier if you use a mailing list. If you find yourself sending emails to the same group of people over and over again, [create a mailing list](#) and avoid having to type each person's email address in each time. Once you log a call with the IT Helpdesk, ICTS will create the mailing list and send you an email containing all your [list's administrative details](#).

As the mailing list owner you now need to make some important security setting changes before you start adding members to your list.

Prevent unwanted people from joining your mailing list by [changing the privacy settings](#). This protects your list members against spam and phishing attempts. You can also decide who can become a list member by [approving or rejecting subscription requests](#).

It is also important to note that if you archive your mailing list messages, anyone who has Internet access will be able to view it. You can avoid this by selecting *Private archiving* in the settings so that only list members will have access to the messages.

Using mailing lists can be quite handy provided you make the necessary security settings. So be on the safe side and rather review your mailing list settings.

#### **Be cautious when using peer-to-peer sharing**

Many South African homes are protected by high walls, security doors, burglar bars and alarms. You could say that, as a nation, we're very aware of security-related issues. Yet how many of us apply that same level of security awareness to our PCs and to the information that we store there?

File-sharing software, protocols such as Direct Connect (DC++), and peer-to-peer (P2P) sites or networks are fertile breeding grounds for malicious software (malware), spyware and adware. In addition, few users of this kind of file-sharing software know how to secure their PCs against attack or are simply unaware of the dangers inherent in its use. If you don't watch out, you could find that confidential work files are accidentally "leaked" or that your personal information is now in the hands of cyber-criminals.

It is risky to use P2P software, but if you are going to use it, at least be aware of its perils and pitfalls and learn how



Projects

Service catalogue

Log a new call

Secure your machine

myUCT

Outlook Web App

Password Self Service

Downloads

NetStorage



Contact us

Like us on Facebook

Follow us on Twitter

entails? Simply put, Grid computing refers to shared computer resources, including High Performance Computing (HPC), between academic and research institutions across the globe. Researchers can use these resources either to process their research results or to solve a computational problems.

South African universities and research institutions are contributing to this service through the SAGrid project which is aimed at providing a national grid computing infrastructure for local and international scientists. Once you [register as a SAGrid user](#), you can log a job request in the workload management system. If there are no resources available in South Africa to process your job, then the system will source a suitable location internationally.

### Need help?

Log a call via our:

- [Online call logging system](#)
- Email: [icts-helpdesk@uct.ac.za](mailto:icts-helpdesk@uct.ac.za)
- Telephone: (021) 650 4500

### Subscribe

If you want to receive this monthly Bits & Bytes newsletter, [subscribe to our icts-newsletter-l](#) mailing list.



### Contact us

Email us your feedback, questions and comments.

FOLLOW US ON [twitter](#)

### More keyboard shortcuts

to mitigate the risks.

- Some peer-to-peer websites are used by criminals to distribute files or viruses that are designed to look exactly like downloads of songs or movies. Apart from the fact that it is illegal to download copyright-protected material, you are risking your security. Ensure that you install McAfee anti-virus and anti-spyware software – on your work and home machines. Keep it up to date!
- Don't accept a P2P program's default installation settings. This is like opening a door to criminals who can gain access to your personal information, files in your folders, and so on. Always manually determine which folders and subfolders will be shared.
- The "browse host" feature in many P2P programmes allows other people to connect directly to your computer and look through file shares. Take extra care when saving private or important files so that you don't accidentally save them to a shared folder. Make sure that you password protect any confidential files.
- In many instances, closing the P2P program (by clicking on the X) doesn't actually close your connection to that network and strangers still have access to your shared folders. When you're finished using the P2P program, use the program's Exit function to ensure that you terminate it correctly.
- If your kids, or anyone else, share your computer, make sure that they have their own user accounts. This will limit any damage to your files and information if they are careless with file-sharing.

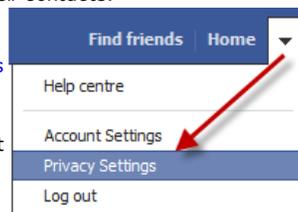
Hopefully you're now a little wiser (and more cautious) about peer-to-peer file-sharing - take care when you share.

### Social networking and personal security settings

Social media sites such as Facebook allow you to share and catch up with people across the globe, but be mindful about how you protect your profile, because you never know who might be reading what you post. Think of it this way: would you stand on stage in front of an enormous crowd (the whole world!) and broadcast your comment or would you much rather share it with a friend over a cup of coffee?

Depending on your Facebook privacy settings - and those of your contacts - anyone can view your profile, read your comments or see your photographs. They could also share your information with their contacts.

It is worth reading the [Privacy Setting Help files](#) on Facebook to understand how to set up Facebook to best suit your privacy requirements.



In addition to the Privacy settings, Facebook now also allows you to change the viewing options at the time of posting a new comment or uploading photos. By default, it will choose the setting that you last used.

Have you ever edited a Word document and then wished you could go back through the document to view your changes? If you forgot to switch on the handy Track Changes feature before making the changes, you can still view them by pressing Shift-F5. Each time you press Shift-F5 it moves the cursor back to the previous change, up to four changes back. It doesn't undo your changes; it just takes you to the spot where you made the change – very useful indeed!

Did you know that you can show or hide the formatting marks used in your Word document by pressing Ctrl-Shift-8? This is the keyboard shortcut for the Show/Hide feature shown on the standard toolbar.

New Facebook users are often confused by the difference between posting to someone's Wall and sending them a Message. When you post a comment on someone else's Facebook wall, everyone to whom they have given access will see your comment. If you want to send them something privately, use the Messages option instead. That way only the two of you see what you wrote.

Twitter has similar privacy settings that allow you to protect your Tweets. You can choose to "Only let people whom I approve follow my Tweets". This will prevent your Tweets from being publicly available.

As the saying goes: "Keep your words sweet and short; you never know when you're going to have to eat them!"

University of Cape Town: Information and Communication Technology Services (ICTS)  
7 Main Road, Mowbray, Cape Town 8000.

Last updated on Thursday, 15 December 2011 @ 11:18 SAST. (Read 1603 times)

 [Printer Friendly Page](#)  [PDF file](#)

#### Related Links

• [PHP HomePage](#) • [HotScripts](#) • [Hewlett Packard](#) • [More about About](#) • [News by Cindy Mathys](#)

#### Most read story about About:

[ICTS Project overview and progress](#)

#### Admin:

[ [Add](#) | [Edit](#) | [Delete](#) ]



© 2016 ICTS - All rights reserved. [Legal Notices](#).  
Last updated 03 October 2016 @ 15:42  
Page Generation: 4.80 Seconds