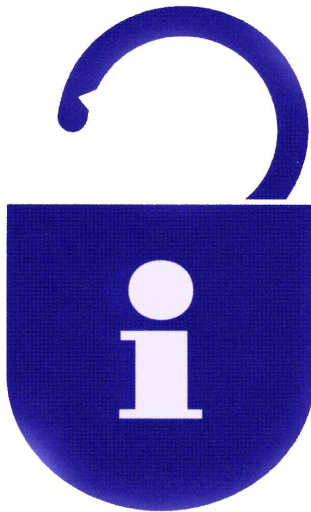


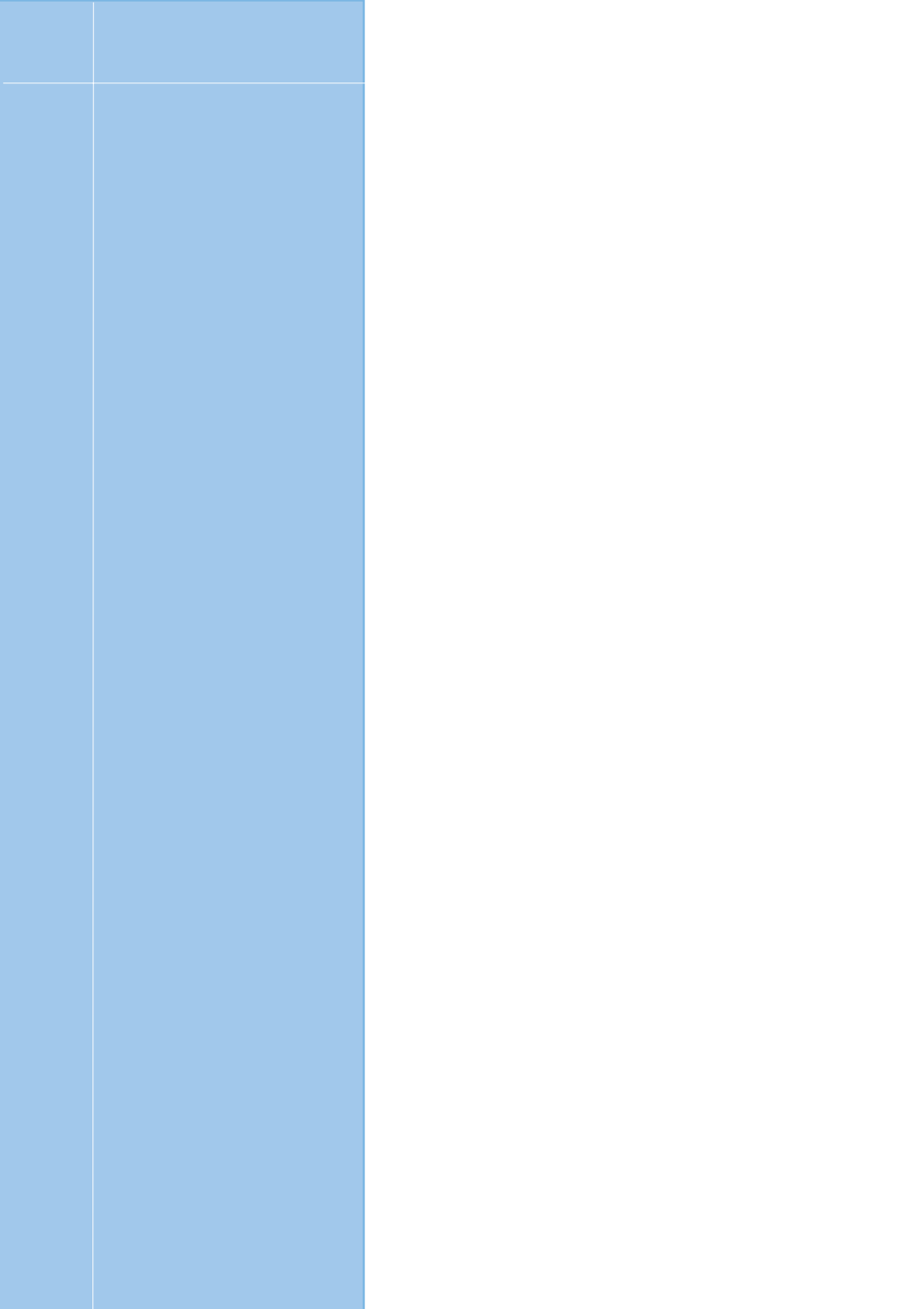
# A Guide to Information Technology Security in Trinity College Dublin



*Produced by*

*The IT Security Officer & Training and Publications  
2003*

Web Address: [www.tcd.ie/ITSecurity](http://www.tcd.ie/ITSecurity)  
Email: [ITSecurity@tcd.ie](mailto:ITSecurity@tcd.ie)



## Contents

What is Information Security	4
Know the Rules	4
A Secure Working Environment for Everyone	5
Secure Communications	5
Processing and Storing Sensitive Information	6
Secure Your Computer	7
Look After Your College Accounts and Passwords	9
Purchasing Computer Equipment	9
Backup Your Files	10
Personal Computers	11
Creating College Websites	11
Keeping the College Network Secure	12
Secure Your Server	12
What's in it for me?	13

## What is Information Security?

Information Security, put simply, is the safeguarding of one of our most valuable assets - the information that is used as part of our core administrative and academic activities here in Trinity College Dublin.

Most of us, whatever our role in College, work with information in many forms. Increasingly we work with information in an electronic format on our computers, on the network, in applications, databases and through electronic mail etc.

This information belongs to the College and our students and it is up to each and every one of us to protect it from unauthorised modification, destruction and disclosure.

This leaflet has been produced by the Information Technology Security Officer at Trinity College Dublin and is designed to show how we can all adopt simple, yet effective, Information Security Practices.

## Know the Rules

There are laws, practices and codes of conduct by which all users of the College IT resources must abide.

The College has recently approved new IT Security Policies. These are available on the IT Security web page. [WWW.TCD.IE/ITSECURITY](http://WWW.TCD.IE/ITSECURITY).

Additionally state laws, for example the Data Protection Act, make the College legally responsible for ensuring that information is accurate and used appropriately.

In addition to fulfilling your legal obligations, complying with the above points will ensure that Trinity College Dublin offers a professional and effective service. Make sure that you are aware of any legal requirements and College policies that apply in your workplace.

And remember, breaking the rules puts us all at risk. By divulging sensitive information, or by not applying strict security controls to sensitive information in your care, you expose the information and the College to potential damage and loss.

## A Secure Working Environment for Everyone

Have you had a good look around your work area lately? Is it safe and secure from intruders and other hazards?

Take a few minutes to check out the security in your office.

- It is up to every staff member to ensure that only authorised personnel enter your workplace. If you see a stranger, do not be afraid to challenge them and request to see their staff or student ID card.
- If it is necessary to bring items home from the office, remember that these should be as secure outside your workplace as they are within it. Please, do not leave important documents or computer equipment, etc. unattended in your car or around the house.
- Operate a clean desk policy. Clear your desk of sensitive items when it is unattended and lock all desks, filing and other cabinets at the end of each working day. Encourage your colleagues to do the same.
- Check what methods are available to dispose of waste materials in your workplace. Items such as old files and computer printouts are very dangerous in the wrong hands. If you are in any doubt, shred it (whilst Trinity is committed to recycling waste paper, remember that Information Security takes precedence).

## Secure Communications

Telephones and email are powerful communication tools, and therefore merit careful use. If you are dealing with anyone by telephone or email, a few basic rules should be followed.

If a person rings up requesting sensitive information...

- Ensure that you are happy they are who they say they are. If in any doubt, phone them back to verify their authenticity using the number you have on file for them.
- Make sure the information that you are quoting is accurate, that they are entitled to know it and that you have the right to disclose it.

If emailing someone...

- Be aware that email is not a secure communication and assume that other people may be able to read it.
- Do not send an email from a TCD email account that states personal views or opinions about other people as this could attract legal ramifications.
- Be aware that email 'header' information can be forged. If you suspect that an email is not from the source it claims to be from then contact your system administrator or the Information Systems Services helpdesk.
- Do not open unsolicited email, especially email with unexpected attachments.

## Processing and Storing Sensitive Information

If you handle sensitive data in your workplace, for example student or staff personal information, medical data, sensitive research data, exam papers or marks, or financial data such as credit card numbers, then you need to take extra care.

Additionally, if you as an individual or as part of your role in College, collect, store and process any data about living people on any type of computer or in a structured filing system then under current Data Protection legislation you are classified as a "data controller" and have responsibilities under the Data Protection Act.

You need to:

- Ensure that your methods of processing, storing and disposing of this information meet the standards set by the College IT Security policies and by the relevant legislation.
- Familiarise yourself with current Data Protection and Freedom of Information legislation.
- If you are purchasing or developing an information system that will process or store sensitive data then you need to be sure that its design and installation meet necessary standards to ensure that the data is protected. The College IT Security Officer can give advice.
- Be aware that information stored on a computer, which is on the College network, is potentially at risk from unauthorised access. Take the necessary steps to protect the information or store it on removable media e.g. zip disk.
- Remember that if you are entrusted with sensitive information then it is up to you to make sure that it remains secure.

## Secure your Computer Today

How private and secure is the information stored on your computer? Can others read or alter your files?

Run through this checklist today to ensure that your computer is protected.

✓ **Make sure you have secure passwords set on all your accounts.**

Blank passwords are the easiest way for an unauthorised individual to gain access to your data. Make sure that all accounts on your computer have secure passwords set.

✓ **Use a password protected screensaver to protect data on your screen.**

Remember never leave your computer signed on while unattended. You are responsible for all actions carried out under your sign-on, so sign-off when leaving your computer.

✓ **Share your files securely.**

You can easily make any folder on your computer available to individuals, groups or to the entire Trinity College Network. Make sure you don't accidentally provide access to more people than you intend! Always share your files to individuals or groups. Never share your files to the 'Everyone' group and always limit 'write' access to your shares, as shared folders with 'write' access can easily become infected by viruses.

✓ **Protect against the destruction caused by viruses by keeping your anti-virus software up-to date.**

Viruses are the most common security problem seen in Trinity College today and the easiest to prevent. Check that you are running the College approved anti-virus software for your area and that it is up-to-date.

✓ **Don't open email attachments from unknown sources.**

Guard against virus infection from unsolicited or spam emails that may be delivered to your account. If you do not know the sender or if you were not expecting the email then do not open the email or its attachments.

✓ **Sign up to Spam Assassin to reduce Spam in your Mailbox**

Spam is unsolicited e-mail on the Internet. It is a form of bulk mail, often sent to a list obtained by companies that specialise in creating e-mail distribution lists. Just as you would throw away junk mail you received in the post you should delete any spam email you receive immediately. Never reply to spam email as this confirms the validity of your email address and may result in you receiving more spam.

The College provides a system to help you deal with spam. Sign up today at <http://mail.tcd.ie/user/anti-spam.shtml>

✓ **Stay current on updates and security patches for your software.**

All software companies are constantly releasing patches and updates to fix security issues, as well as other flaws discovered in their products. These flaws are what virus writers and hackers exploit to gain access to your data. Make sure you stay ahead of the hackers and keep your software up-to-date. A quick and easy way to update your Microsoft software is to run “Windows Update” from the icon on your start menu.

✓ **Don't give out your email address or any information regarding your PC to unknown individuals.**

Do not provide details on your computer or any of your College account information to other individuals. Help prevent spam email by not giving out your College email address on Internet sites.

✓ **Don't download suspicious material from the Internet**

Be careful when you are out browsing the Internet; don't give personal details out on public web sites. Be careful when downloading files, always scan downloaded files for viruses.

✓ **Make sure you only install legally licensed software on your PC**

Be conscious of software copyright and under no circumstances make unauthorised copies. Only use software that is approved and has been verified by the College as being virus free.

Do you think you are missing any of these crucial security checks? Then visit [www.tcd.ie/ITSecurity](http://www.tcd.ie/ITSecurity) for further information on how to secure your computer.

## Look After your User Accounts and Passwords

Your username and passwords allow access to College resources. They also protect College data from access from unauthorised individuals both internally (other staff students) and externally (hackers!)

Therefore it is vital that you:

- Keep your password secret.
- Change your password regularly (at least twice a year).
- Do not write your password down anywhere!
- Change your password immediately if you suspect it has become known to others.
- Make your password complex and hard to guess

How to choose a good password?

Your password should be at least six characters long and contain both letters and numbers. A good password is difficult to guess so:

- Do not use your name, nickname, initials, user ID or staff/student number or telephone number.
- Do not use dates, especially ones that are readily available such as your date of birth.
- Do not use consecutive keys on a keyboard, e.g. ASDFGH or all the same characters, e.g. 111111 or KKKKKKK.
- Do not use words that appear in a dictionary, or proper names.
- Combine letters and numbers/symbols such as taking the first character of every word in a sentence e.g. "I go home to Cork very weekend" would be "Igh2Cew".

Keeping your password secret protects you from unauthorised actions being carried out under your personal sign-on. Do not divulge it to anyone!

## When Purchasing Computer Equipment

When purchasing computer equipment place your order with the College preferred suppliers as listed at <http://isservices.tcd.ie/purchase/index.html>

When you buy from these sources you receive hardware that has been carefully selected via an official tendering process.

Also the computer you receive will be securely configured with all the software you need to get started.

## Backup your Files



Ask yourself the question -

‘What would I do if my computer was stolen today, or I lost everything during a system crash tomorrow?’

Then act on the answer!

Backing up your files means making a spare copy of every file stored on your computer’s hard drive, which you have created or modified. Make a list of all your important documents and data and decide how you will back them up today!

If you are responsible for a collection of data held either remotely on a server or on the hard disk of a computer, you should consult your departmental System Administrator or Information Systems Services regarding the existence of local back-up procedures.

Do not assume that someone else is backing up your data. Unless you have made explicit arrangements for your data to be backed up then it probably is not being backed up.

Your backup is your responsibility and should be:

- Comprehensive – Make sure you are backing up all the files that you own and don’t forget to backup your email inbox.
- Timely - You should back up all-important files before your computer is repaired or has new software installed or has any major hardware or software upgrades.
- Regular - You should back up your files according to a regular schedule (e.g., every Friday afternoon). Schedule backups of sensitive information daily.
- Secure - Your backup should be kept in a separate, secure, fireproof area and all copies and backups should be handled with the same care as the originals.

Familiarise yourself with backup and retrieval procedures for your information today.

## Personal Computers

If you connect a personal computer to the College network you need to ensure that it meets the same high security standards as computers owned by the College. Similarly, if you use a College owned laptop computer at home or while travelling on College business you need to ensure the security of the computer and the data stored on it.

Make sure you:

- Register your personal computer with Information Systems Services or your local System Administrator.
- Install anti-virus software on your personal computer. The College anti-virus licensing arrangement covers personal computers when they are used to connect to the College network.
- If you are dialling up to the Internet from home or elsewhere using a commercial ISP then use a personal Firewall to protect your computer from dangers on the Internet.

Consult your local administrator or Information Systems Service for more information.

## Creating College Web Sites

If you are responsible for creating or updating web sites, which represent the College, be aware that the College may be put at risk by the content displayed on these web sites. Where content is incorrect, defamatory or illegal the College could be at risk from financial loss from resulting legal proceedings.

So make sure that:

- You never share your web authoring username and password with anyone else.
- You check the accuracy of all information you post on official College web sites.
- You check that the information you publish is legal and does not contain defamatory comments about individuals or organisations.
- If you are collecting information via a College web site make sure that your means of collecting, processing and storing the data meet the standards in the College policies and all relevant legislation.

## Keep the College Network Secure

The Trinity College data network consists of an interconnection of approximately 10,000-networked devices. These include computers, printers, network cables and other networking equipment.

Any one of these devices can impact on the performance and availability of the network services which we all use.

Additionally, networking devices such as hubs, switches and wireless access points when connected to the College network can provide unauthorised access to the College data networks to third parties.

It is therefore essential that we maintain a record of all devices connected to the network, where they connect and who is responsible for them.

Help us maintain the security of the College network by:

- Registering all devices with Information Systems Services at <http://isservices.tcd.ie/help/connect/index.html> before you connect them to the network.
- Registering all devices with your local System Administrator if you are located on the Computer Science, Maths, or Electronic and Electrical Engineering data networks.

## Secure Your Server

If you run or are responsible for maintaining a College Server be aware that your server could be potentially at risk from hacking activity and viruses particularly if your server is accessible from the Internet.

When security on a server is compromised the highly sensitive data stored on the College network such as employee data, student data, research data and financial information is put at risk. Data can be lost, altered, or stolen, and the College could suffer serious consequences.

Take steps to secure your server today!

## What's in it for me?

There is something in it for all of us. The continuing success of the University depends on the confidentiality, integrity and availability of our information.

As we now know, the responsibility for safeguarding that information rests equally with each one of us.

Closer to home however, following the basic security practices, which we have discussed, can improve your working life on a daily basis.

- For instance, adopt a clean desk policy and see how quickly you begin to notice the benefits an orderly and uncluttered working environment brings!
- Take to heart the points mentioned in the section on backup, remembering that, if disaster does strike, you are in a good position to deal with it.
- Remember a well chosen, secret, password ensures that nothing will be done in your name by somebody else.

Good Information Security can be achieved through basic steps that do not require any special knowledge or skills. "If in doubt, just use common sense."

## Any questions?

If you need more information, contact the College IT Security Officer at [ITSecurity@tcd.ie](mailto:ITSecurity@tcd.ie) or visit the new IT Security website at [WWW.TCD.IE/ITSecurity](http://WWW.TCD.IE/ITSecurity)





