



Keeping Information Secure

A University guide on how to keep your important work safe

January 2012
Information Systems & Services
Newcastle University

Index

1.0 Understanding Information Security

1.1 What is information security?	3
1.2 Why is information security important?	3
1.3 What are the threats?	3
1.4 What steps can we take to protect information?	4

2.0 Accessing ICT Services

2.1 Your computer account	5
2.2 Your university smart card	5
2.3 ICT policy	5

3.0 Protecting your Data and Devices

3.1 Saving your work	6
3.2 Data disposal	6
3.3 Office security	6
3.4 Mobile working	7

4.0 Encryption

4.1 What is encryption?	8
4.2 Recommended encryption products	8
4.3 Devices that cannot be encrypted	9
4.4 Other important points to remember about encryption	9

5.0 Scam Emails

5.1 Protect yourself from scam emails	10
---	----

6.0 Email and Internet

6.1 Email and Internet	12
6.2 Cloud computing	12
6.3 Copyright materials	13
6.4 Monitoring and logging	13

7.0 Protecting ICT Services

7.1 Viruses and Malicious software	14
7.2 Lost and found items	14
7.3 University managed computing devices	14
7.4 Security incidents	15

1.0 Understanding Information Security

1.1 What is information security?

Information security refers to the steps that we can take to:

- Ensure good data management.
- Protect information against damage, loss and theft.
- Protect the ICT equipment and systems used to collect, store and process that information.

1.2 Why is information security important?

Certain types of information are legally protected under the Data Protection Act (e.g. staff, student and medical records). Other types of information may be protected by a contractual agreement (e.g. financial or commercially sensitive data provided by a private sector company).

A failure to safeguard other people's personal information may cause them serious distress. In some cases, those people may become victims of crime. Negative publicity and regulatory action by the Information Commissioner's Office may also cause significant damage to the reputation of the University.

A failure to safeguard information that is protected by a contractual agreement may result in the University being refused access to important research funding and research data. Such an event may impact the University's ability to carry out research.

1.3 What are the threats?

The types of threat that may result in the damage, loss and theft of protected information include:

- Loss and theft of portable computing devices (e.g. laptops, tablet computers and smart phones) and portable storage devices (e.g. USB flash drives and external hard disk drives).
- The accidental publishing of confidential information on the Internet (e.g. social media, blogs and messaging boards).
- The sending of a confidential email to the wrong recipient.
- Large volumes of confidential printed information kept on desks.
- Confidential documents left on photocopiers and fax machines.
- Unlocked filing cabinets.

Keeping Information Secure

- Incorrect disposal of confidential information (e.g. failure to shred confidential paper waste, failure to securely erase computer data).
- Non-secure cloud computing (e.g. cloud service may be located in a country with no data protection laws).
- Scam emails sent by criminals in an attempt to obtain important personal information.
- Viruses and malicious software.
- Computer hackers.

Personal information is valued by criminals who will steal it for fraudulent purposes. In 2010 the National Fraud Authority revealed that £1.9bn was fraudulently obtained in the UK through the theft of 1.8 million identities, averaging over £1000 for each victim.

PricewaterhouseCoopers revealed in their 2008 Information Security Breaches Survey that the loss and theft of portable computing devices and portable storage devices is a major cause of information security breaches in the work place.

1.4 What steps can we take to protect information?

By following the guidance contained in this document, you can help reduce the risk of information being damaged, lost or stolen.

2.0 Accessing ICT Services

2.1 Your computer account

Prevent unauthorised access to your work and email by keeping your user ID and password safe.

Remember:

- You are responsible for all use of your computer account.
- Never allow anybody to use your computer account.
- Never tell anyone your password, even if they are University staff.
- Never leave a logged on computer unattended. Lock your computer if leaving it for a short time. Log-off your computer if you are leaving it for longer.
- If you think somebody else has logged on as you, immediately change your password and notify the ISS Service Desk by telephone on +44 (0) 191 222 5999 (external) 5999 (internal) or by email to helpline@ncl.ac.uk
- Keep your password secret and change it at least every three months.
- Make sure your password is at least eight characters long, not based on a dictionary word, includes a mix of upper-case and lower-case letters, and a mix of alphabetic, numeric and special characters. An example password is Ncl*2011.
- Keep your password hidden if you need to write it down.

2.2 Your University smart card

Your smart card is unique to you and enables you to access controlled learning resources and buildings.

Remember:

- You are responsible for all use of your smart card.
- Never allow anybody else to use your smart card.
- If your smart card is lost or stolen, immediately notify *Nu SMART Card Returns* by telephone on +44 (0) 191 222 6060 (external) 6060 (internal).

2.3 ICT Policy

ICT policies governing use of the University's ICT systems are available to download at:

- <http://www.ncl.ac.uk/iss/policy/>

3.0 Protecting your data and devices

3.1 Saving your work

Your home-drive is located on the ISS filestore and is backed up on a regular basis. This makes it possible for ISS to recover your work if any of your files are accidentally damaged or lost.

Remember:

- Save all work to the ISS filestore.

3.2 Data disposal

If your work is commercially sensitive, or contains other peoples personal information, it will need to be disposed of securely.

Remember:

- It is possible to recover electronic information stored on a computing device unless you use secure deletion software. ISS can advise on suitable secure deletion products.
- To dispose of confidential paper records, either shred them or deposit them in a confidential waste bag.

3.3 Office security

Take steps to prevent the loss and theft of data and devices in your work area.

Remember:

- Do not let unauthorised people follow you through a locked door if they do not have a Newcastle University smart card or visitors pass.
- Minimise the amount of confidential printed information you keep on your desk.
- Immediately collect all confidential print jobs and faxes. Do not leave confidential information on a photocopier or fax machine unattended.
- Keep all mobile computing devices, mobile storage devices, and other valuable items in a secure cabinet or drawer if they are not in use.
- Store your confidential printed information in a locked drawer or filing cabinet at the end of each day.
- Do not leave an unattended filing cabinet unlocked.
- Make sure all doors and windows are securely closed if you are the last person to leave your work area.

3.4 Mobile working

If you work away from the University or in a non-secure work area (such as a coffee shop, public park or train), take steps to prevent the loss, theft and damage of your valuable items (including your mobile computing devices and portable storage devices).

Remember:

- Try to be discrete when carrying high value items.
- Do not leave high value items unattended in a public space or motor vehicle.
- Position your devices so that people cannot see what is displayed on your screen.
- Do not let people see you type your password.
- If possible, work through the [ISS Remote Access System](#) instead of saving your work to a mobile computing device or portable storage device.
- If it is not possible to connect to the ISS Remote Access System, then encrypt your electronic work.
- Before you encrypt your work, back it up to the ISS filestore. This will ensure your work can be recovered if it is damaged, lost or stolen.
- Before you leave, check that you have all your personal belongings.

4.0 Encryption

4.1 What is Encryption?

Encryption refers to the process of converting your information into a form that cannot be understood by anyone who is not permitted to view that information. Without encryption it is very easy for a criminal, such as a computer hacker or an identity thief, to intercept and view your work.

Encryption should be used to protect against the loss and theft of valuable information when it is:

- Stored on portable computing devices such as laptops, tablets and smart phones.
- Stored on portable storage devices such as USB flash drives and external hard disk drives.
- Sent as an email attachment.
- Sent across the Internet.

The types of information you should encrypt includes:

- Personal information that is protected under the Data Protection Act (e.g. staff, student and medical data).
- Information that is protected by a contractual agreement (e.g. financial or commercially sensitive data provided by a private sector company).

4.2 Recommended encryption products

If storing protected information on:

- **A Windows computer**
Encrypt that information with [Microsoft Bitlocker](#).
- **A Linux computer**
Encrypt that information with [TrueCrypt](#) if no built in encryption is available.
- **An Apple Macintosh**
Encrypt that information with [Apple FileVault](#).
- **A portable storage device**
Use a USB data stick or hard disk drive that provides AES-256 encryption. The ISS Information Security Team can advise on which devices to use.

If sending protected information via:

- **Email**
Protect that information using the AES-256 encryption capabilities built into [7-Zip](#) and [WinZip](#). Both products can be used to create encrypted ZIP file archives that can be attached to an email.

- **The Internet**
Contact the ISS Information Security Team for guidance on appropriate solutions such as Secure File Transfer Protocol (SFTP).

If you are a member of staff, the ISS Service Desk or your local computing officer can arrange installation and configuration of these encryption products. If you are a student, further guidance is available from the organisation that created the encryption product.

4.3 Devices that cannot be encrypted

It is not always possible to encrypt the newer types of mobile computing device, such as tablets and smart phones. It is recommended that you seek advice from the ISS Information Security Team before storing information on these types of devices.

4.4 Other important points to remember about encryption

- It is not possible to recover your information should anything go wrong during the encryption process or if you forget your encryption passphrase or lose your encryption key. Always keep a non-encrypted master copy of your valuable information on the ISS Filestore.
- Do not store protected information on a portable computing device or portable storage device, or send that information by email or via the Internet, unless absolutely necessary.
- If you have no other option but to store protected information on a portable computing device or portable storage device, keep that information to a minimum.
- Protected information should only be stored on a portable computing device as a temporary measure (e.g. if it is not possible to use the ISS Remote Access System).
- You should only store protected information on a portable storage device for data transfer purposes, and when no other secure data transfer method is available.
- Remove all protected information from the portable computing device or portable storage device if it no longer needs to be kept on the device.
- Just like your bank card and PIN, never store your encryption passphrase or key with your encrypted information.
- Use a long encryption passphrase that is at least ten characters long and contains a mix of alphabetic, numeric and punctuation characters. An example of such a passphrase is: **“I’ve worked in HE for 3 years!”**
- Always keep a record of the devices that you have encrypted. This will allow you to confirm if a device was encrypted if it is lost or stolen.

5.0 Scam emails

5.1 Protect yourself from scam emails

Criminals are sending scam emails that fraudulently claim to be from the University. Criminals also send scam emails that fraudulently claim to be from banks and credit card companies, on-line retailers and other service providers such as web-mail and social networks. Some of these scam emails will falsely offer you money, unclaimed inheritance, consumer goods, unclaimed prizes and employment opportunities to lure you in.

The majority of scam emails are blocked by the University, however some emails will still get past our security systems as criminals adopt increasingly sophisticated methods of attack.

These scam emails attempt to trick you into providing important personal information such as your username, password, bank account logon details, credit card number, date of birth, and other information that may be useful to a fraudster.

Criminals want this information to:

- Access and steal money from your online bank account
- Commit credit card fraud
- Steal your identity
- Send fraudulent emails from your computer account
- Access your confidential work

Criminals may try to trick you into opening an attachment contained in the scam email. This attachment may contain spyware (a malicious type of computer program) that can record the web sites that you visit, record the usernames and passwords you type to log-on to those web sites, and copy the private files stored on your computer and network drive. The email attachment may contain other malicious computer programs, such as worms, that are used to attack other computers on your local network and the Internet.

The email may contain a web address that looks correct, but will take you to a fake web site. The fake web site may look identical or very similar to the web site of the organisation that the email fraudulently claims to be from.

Your personal information is valuable to criminals. The damage caused by criminals using your personal information can be very difficult to repair and may cause significant distress.

Protect yourself by remembering these simple rules:

- The University will never ask you for your password.
- If you receive an email that asks for your password, internet banking log-on details or credit card number, it will be a scam.

Keeping Information Secure

- If you receive an email that offers something that is too good to be true such as a free gift, money, or an unclaimed inheritance, then it will probably be a scam.
- Do not respond to the email, open any attachments, or click on any web addresses contained in the email.
- Delete the email.
- If you have accidentally provided any passwords, change them immediately.
- If you have accidentally provided your internet banking log-on details, change them immediately and notify your bank for further advice.
- If you have accidentally provided your credit card number, immediately notify your credit card company for further advice.
- Take precautions to stop malicious software infecting your computer.

Further advice on protecting yourself from identity theft is available from the [Information Commissioner's Office](#).

6.0 Email and Internet

6.1 Email and Internet

The University provides email and Internet to support your University work.

Remember:

- Use these facilities in a lawful, ethical and considerate way.
- Do not engage in activity that would impact the quality of these services for other users.
- Do not send other peoples personal information, or any commercially sensitive information, via email or the Internet unless encrypted. ISS can advise on suitable encryption products.
- Before sending an email, always double check the email address of the person you are sending to.
- If sending an email to multiple recipients, and those recipients do not need to know each other's email address, use Blind Carbon Copy (BCC) instead of Carbon Copy (CC).
- Stay alert for scam emails.

6.2 Cloud computing

The cloud is made up of web-based services that you can use to store and process your work. These services include file-storage, web-mail, office applications, social networking, social media, and special purpose web-applications.

Remember:

- Never upload other peoples personal data to a cloud-based service.
- Always check the terms and conditions before using a cloud-based service.
- You may no longer have exclusive control over your work after it has been uploaded.
- Your work may be unavailable or non-recoverable if the cloud-based service ceases trading or experiences a technical problem.
- You may not be able to remove your work after it has been uploaded.
- The cloud-based service may be based in a country that has no laws to protect your data.
- Before you upload your work to the cloud, back it up to the ISS filestore.
- Use a different password for each cloud-based service.

6.3 Copyright materials

Do not illegally download or share copyright materials such as music, movies and computer games.

Remember:

- Copyright holders have ways of detecting illegal activity.
- Copyright holders will notify ISS of illegal activity traced to devices connected to the University's network.

6.4 Monitoring and logging

In compliance with University ICT policy, ISS legally monitors and logs activity that occurs on the University's network.

7.0 Protecting ICT Services

7.1 Viruses and malicious software

Viruses and malicious software are capable of destroying your work, stealing your personal information, and disrupting your access to ICT services.

If using your own computing devices, remember:

- Protect yourself from viruses and malicious software.
- Install the latest security updates for your operating system and applications.
- Install anti-virus software on your computer and keep it up to date.
- Virus-scan all email attachments, removable media and files downloaded off the Internet.
- Run a personal firewall that will let you know if a suspicious program tries to access the Internet.
- Do not operate your computer as a local administrator unless you need to install software.
- Do not download or install any software from an unknown or un-trusted source.

7.2 Lost and found items

If you find any items that appear to have been lost, such as a mobile computing device or removable media, remember:

- Never attempt to connect a found device to your own computer or a University-managed computer. The device may contain a virus or other type of malicious software.
- Hand the found device into the ISS Service Desk so that we can attempt to identify the owner.

7.3 University managed computing devices

All computing devices provided by the University are there to assist you in your work. Please treat these devices with respect.

Remember:

- Do not attempt to modify these devices in any way. Doing so may impact the ICT service.
- Only connect USB devices that are powered through the USB port.

Keeping Information Secure

- Remain vigilant for any suspicious devices.
- Report all suspicious devices to the local Computing Officer.

7.4 Security incidents

If you discover anything that you believe poses a risk to the security of University ICT systems, contact the IT Service Desk by telephone on +44 (0) 191 222 5999 (external) 5999 (internal) or by email to it.servicedesk@ncl.ac.uk