Lancaster University
Information Security Policy and Processes

Information Security Policy

1. Introduction

This document defines how we (Lancaster University) will manage our Information Security practices. Mismanagement of information can result in serious harm to the University's reputation and day-to-day operations.

The aims of this Information Security policy and associated processes are:

1. To ensure University Information Assets and IT Infrastructure are not misused.
2. To ensure everyone understands their responsibilities with respect to Information Security.
3. To minimize the likelihood of an Information Security breach or accidental loss of data by ensuring that everyone takes Information Security seriously.
4. To make sure we meet our legal requirements with respect to Information Security, which includes the legislative frameworks of the Data Protection Act and the Freedom of Information Act.

Information Security's core principles are confidentiality, integrity and availability; this document identifies the policies and processes that we use to ensure the confidentiality, integrity and availability of the University's information.

- **Confidentiality:** ensuring that only those who ought to be able to access information can do so
- **Integrity:** ensuring that information cannot be modified without that modification being detected
- **Availability:** ensuring that the information can be accessed when it is needed.

The document is split into sections describing high level policy, and then further sections describing both mandatory and advisory processes. Everyone with a particular role must follow the mandatory processes for that role, and it is recommended that they also follow the advisory processes.

The policy and processes below aim to enforce the mandate given in the Rules of the University[1] (within the Computer user Agreement, Appendix C) The policy and associated processes align and must remain aligned with the JANET Acceptable Use Policy[2].

[1] https://gap.lancs.ac.uk/policy-info-guide/5-policies-procedures/rules-of-the-university/Pages/default.aspx
[2] https://community.ja.net/library/acceptable-use-policy

2. Everyone

2.1 Keeping Information Secure

We all want to keep the University's information secure; the consequences[3] can be significant for all or any of us if we don't. We all have a role to play in this task; some of us have greater roles than others. We all recognise the broad areas of Policy in this document that defines our institutional approach to information security.

The consequences for an individual of not adhering to this institutional policy on information security are significant. For a breach considered wilful with significant institutional implications, resultant disciplinary action could include dismissal. In circumstances where legislation is not followed, legal action could be taken.

This Information Security Policy is aligned with the good industry practice and controls as defined in the ISO27000 family of standards.

2.2 Groups with Specific Responsibilities

There are also some groups with special responsibilities and they are listed here:

- IT Professionals
- Secretariat
- Human Resources
- Heads of Department and Data Custodians

Users Handiling or Processing PaymentsThe responsibilities which relate to those roles are described in later sections.

For contractual or legal reasons, or due to other obligations, your department may have additional information security policies or guidelines to which you must adhere; it is the Head of Department's responsibility to make you aware of them.

2.3 Stay Up-to-Date

We need to review this document periodically and keep it up-to-date as the law or University policy changes. There is a section on the relevant law below.

We'll rely on ISS to keep us informed and advise us what we need to do to keep information secure. The Information Security Foresight Group will assist and advise. We'll follow the processes that ISS publishes.

To make sure that the information security policy and associated processes remain fit for purpose, they will be reviewed on the following schedule:

- Review of the Information Security Policy – 3 years (amendments to be approved by ITPC)
- Review of Mandatory Processes 1-2 years (amendments to be approved by Information Security Foresight Group)
- Review of Advisory Processes – 0.5-1 year (amendments to be approved by Information Security Foresight Group)

[3] The consequences for the institution in terms of reputational loss are incalculable; but significant fines could be imposed were it determined that we did not take reasonable steps to secure information, or acted in such a way that we knowingly put Information Security at risk. The University could face a fine as high as £500,000.

Periodically, ISS will use outside auditors to track our progress.

2.4 Information Systems

ISS keeps a list of systems that hold information which needs to be managed securely. They'll make sure that the owners of those systems know what their Data Custodian responsibilities are. Owners need to declare to ISS (through the Information Security Foresight Group) that such systems exist and make it clear to ISS how each system's information should be categorised.

The University is required by law to notify the Information Commissioner's Office of any significant information security breach. We all recognise that the Institution would need to deal with the subsequent professional, social and publicity-related issues surrounding such a breach.

Some of the University's information is on paper, and it is just as important to keep that safe. We will not print restricted or personal data unless this is necessary, and when we do so we will be responsible for ensuring it is recycled with confidential waste or shredded.

2.5 Keeping Information

We will all keep our information for no longer than necessary, and follow the University's published retention schedule[4] for the information we hold. We also follow the Records Management guidance provided and keep our knowledge up to date by attending relevant training as necessary to ensure we look after our information properly.

3. IT Professionals

"IT Professional" means Information System Services personnel and Departmental staff who are Systems Administrators for any shared computer on the network or application developers.

There are some things that IT Professionals need to do to keep information secure:

- IT Professionals will be familiar with the ISO27000 family of standards and controls for Information Security, and will adopt or adapt that good practice in their work at this University.5
- They will proactively manage risk. ISS can help with Information Security Risk Assessments and identify the controls that will help keep data safe.
- IT Professionals will always follow a change management process when making changes to the way we manage secure data. That change management process will ensure the on-going integrity of the secure data.
- IT Professionals will keep everyone informed about our Information Security policy.
- IT Professionals will respond to potential threats identified through remote scanning of suspect devices; with the authorisation of the Director of ISS, such responses may include removal of those suspect devices from the network.
- IT Professionals will maintain a variety of technical controls to ensure the security of the IT infrastructure and systems. The list of technical controls should be documented.[6]

Clearly, the institutional standards for secure systems administration, systems and applications development, and security monitoring and interventions that are followed by IT Professionals constitute

[4] https://gap.lancs.ac.uk/Records%20Management/Retention/Pages/default.aspx
[5] The Information Security Foresight Group can provide access to the University's copy of the standard.
[6] Technical Controls implemented centrally by ISS are published online at http://www.lancs.ac.uk/iss/security/Information_Security_Technical_Controls

a large manual in its own right. Through consultation with staff and security professionals, ISS will define an Institutional Standards Handbook that IT professionals are required to follow in order to maintain institutional information security.

4. Strategic Planning and Governance

Information Security is an important part of processing personal data in compliance with the Data Protection Principles.

The Information Compliance Team of Strategic Planning and Governance will provide training and advice to University staff on Records Management and compliance with information legislation such as the Data Protection Act and the Freedom of Information Act.

5. Human Resources

We can rely on the Human Resources department to ensure that people joining the University or changing their role within the university are made aware of their responsibilities when it comes to Information Security.

To ensure we know people are who they say they are, Human Resources ensure that all employees are legally entited to work, by confirming their identity against their passport; they also ensure that we have at least one reference for new employees.

Human Resources ensure that employees and contractors terms and conditions of employment require adherence to this policy, and risk disciplinary action if this policy is not followed. The standard disciplinary processes are followed in the case of breaches of the information security policy.

Information Security training objectives will focus on the processes within this policy. Training successfully completed by staff will be recorded on the central Human Resources system.

When a member of staff leaves the university or a contractor's contract is terminated, Human Resources will make sure their record reflects when they left, to ensure that they no longer have access to university systems. Any information assets that are restricted or personal that are in the possession of that member of staff or contractor must be returned to the University – the responsibility for its return is held by the department for which they worked.

6. Users Handling or Processing Payments

Users that are required to handle or process credit card information as part of their role within the University have additional responsibilities as part of the universities ongoing compliance with the Payment Card Industry Data Security Standard (PCI DSS). All users must ensure they complete the PCI DSS training prior to handling card data and renew the training annually.

They must also familiarise themselves with additional policies, specific to payment card handling.

7. Heads of Department and Data Custodians

Heads of Department will maintain a list of systems under their control that contain restricted or personal information. A Head of Department may delegate that responsibility to Data Custodians assigned to different information assets.

If there is any suspicion that there has been a breach of information security in any of those systems, that Head of Department will:

1. Do what he or she can to find out exactly what happened
2. Ensure that the right things happen to inform people what has happened
3. Make changes to ensure it does not happen again.

We rely on Heads of Department to have an open door policy so that they can:

- Let ISS know if they suspect a system containing restricted or personal information has been compromised or misused.
- Let ISS know of new systems that contain restricted or personal information so that ISS can maintain the list of such systems and offer help and advice in securing them.

8. Heads of Department are also responsible for ensuring that departmental processes and practices comply with this policy. They must ensure that staff are aware of their individual responsibilities and obligations, encouraging them to follow the processes and take part in training when appropriate.Relevant Law

There are a number of laws which relate to our use of computer resources; some things that we might do may not only breach our security policy, they may also be illegal. ISS guidance will help you comply with this legislation, and pointers to published material will help you access it in greater detail. To help spread a greater level of understanding of the relevant legislation, ISS will work with Human Resources to offer a programme of workshop events.

The Counter Terrorism and Security Act 2015 imposes a duty on Higher Education bodies to engage with the Prevent Duty. This duty requires Universities to have 'due regard to the need to prevent people from being drawn into terrorism'. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The University reserves the right to block or monitor access to such material.

The relevant law can be found at, for example:

The Copyright, Designs and Patents Act (1988)
http://www.legislation.gov.uk/ukpga/1988/48/contents

The Data Protection Act (1998)
http://www.legislation.gov.uk/ukpga/1998/29/contents

The Computer Misuse Act (1990)
http://www.legislation.gov.uk/ukpga/1990/18/contents

Obscene Publication Act 1959 & 1964
http://www.legislation.gov.uk/ukpga/1964/74/contents

Regulation of Investigatory Powers Act 2000
http://www.legislation.gov.uk/ukpga/2000/23/contents

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Prevent Duty Guidance: for higher education instituions in Engalnd and Wales
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf

Information Security Processes

Further to the University's Information Security Policy, these pages provide specific processes which ensure we keep information safe at the university. We must all follow these processes to maintain our shared responsibility for keeping the university's information safe.

Mandatory processes are distinguished from advice through formatting. Mandatory processes are in the following format:

> **The text in this box describes a mandatory process**

Processes

- Information Classification
- Encryption
- Passwords
- Safe Browsing
- Protection from Common Internet Threats
- Use of Cloud Services
- Use of Social Networking TOols
- Basic Computer Safety
- Disposal of Media
- Information Security and Systems Development
- Legal Framework and Privacy

1. Information Classification

Information is valuable; we classify information so we know how to protect it. It is easy to forget how much information we can carry with us when it is electronic.

Some big, very public losses of data have changed how much attention is being paid to electronic information. Breaches of the Data Protection Act can be very costly for both the individual and for the institution.

It is important to understand what the University means by ordinary, confidential, restricted and personal information and what the consequences for loss of that information may be. Some data, though not necessarily categorised as restricted or personal, may still be very valuable and needs to be protected: data collected as part of a research project, for example; so both the value and the classification of data should direct how we secure that data.

The Secretariat has a definitive policy document "Policy on Categorising and Protecting University Information Assets"[7]. Furthermore, clauses 2.18 and 2.19 of the University Rules (Disciplinary Breaches) identifies breaches relating to elements of University business that are 'Restricted' or breaches that relate to 'Personal Data'.

[7] http://www.lancs.ac.uk/depts/recman/docs/SEC-2011-4-0009-Policy-on-Categorising-and-Protecting-University-Information-Assets.docx

Access to Restricted or Personal data must be limited to the minimum required to perform the required task.

Restricted or Personal data must not be downloaded or copied to mobile devices unless the device is capable of appropriately encrypting the information.

We know that it is safest to use university equipment only for university business.

If you are travelling and you will need access to restricted data, speak to ISS about borrowing a secured laptop, or taking a 3G device to use for remote access

Additional Responsibilities for Data Custodians

To ensure the security of information classified as restricted or personal, Data Custodians have certain additional responsibilities, described below.

If you control a source of Restricted or Personal data for use by a group of people, you need to act as Data Custodian for that data; ensuring that only those people who ought to have access to the data do so, and reporting any breaches of the security of that data. When you keep a copy of restricted data locally, you must act as the Data Custodian of that data.

Data Custodians need to ensure that data is secured against accidental disclosure and intentional attempts to access their system. Restricted information must be secured using at least access control lists (ACLs) as well as encryption and any protection offered directly by the application that stores the restricted information.

2. Encryption

Encryption is a powerful tool to secure information; certain types of University information must be encrypted. The section on information classification above explains which data must be encrypted.

Encrypt all Restricted or personal data on your computer; laptop; mobile phone; CD; DVD; external hard-disk drive, USB Stick or other data-holding device.

When sending email; copying data onto, for example, CDs, laptops, phones or USB sticks; or when working outside the confines of the University you must secure information appropriately.

When working with restricted information away from the University you must always use a secure mechanism such as VPN or Remote Desktop Access. [8]When it is not possible, you *must* **ENCRYPT personal information. For the avoidance of doubt, all laptop data must be encrypted as it is unlikely that a laptop can be guaranteed to be free of Personal or Restricted information.**

ISS are happy to help with encryption; call ISS Service Desk to arrange for an ISS technician to encrypt your laptop.

[8] If you are not certain whether a particular access mechanism is secure, ask ISS.

3. Passwords

Nothing can guarantee the security of our passwords, on campus or anywhere else; the use of public access PCs represents a threat, as does using any other PC which might record keystrokes through a keylogger. However, the following mandatory processes significantly increase password security.

Do not share your University password with anyone. We protect ourselves and our colleagues if we never share passwords. If someone asks you to share your password, it is always OK politely to say no.

Passwords must be:

- **Easy for you to remember**
- **Difficult for others to guess**
- **Kept secret and never shared with *anyone* for *any* reason**
- **Made up of upper- and lower-case letters, numbers and symbols**

ISS staff never need to ask for your passwords, and no one else needs to either. When you do need to share information, contact ISS for easy ways to do so without sharing passwords.

Contact ISS for more advice and information on more general password management, including the management of passwords for non-University systems, and the use of third-party products and services to manage passwords.

4. Safe Browsing

This section provides examples of common dangers that face users of the Internet and how to protect against them. Here are some things that you can do to make sure that you are always well protected:

Do not access important information like your University email from shared computers that you cannot trust (for example, cyber-cafes and other public computers). It is far too easy for your login details to be covertly copied.

Do not allow your web browser to save or remember your University Login details.

Do not re-use your University email address and password for other accounts.

Make sure your PC has acceptable anti-virus software installed, keeps its definitions up-to-date and runs a scan at least once a week. If you are unsure of any of the results of a scan contact your Departmental IT Support.

- Keep your computer and your web browser up-to-date. The University's Managed PC service will do this for you.
- Make sure web browser plugins like Flash and Java are kept up-to-date.
- Never use wireless networks if you do not know who is responsible for them. Creating a fake "free Internet access" wireless network offering is a commonly used way to detect passwords and capture your Internet traffic.

Web browser toolbars and other add-ons: There is a wealth of helpful software available to install in your web browser that is designed to help you use search engines or block pop-ups etc. However not all of this software can be trusted and may contain keyloggers, viruses or Trojans designed to steal your information or force you to visit specific web pages.

Please apply the following rules when selecting web browser add-ons;

- Only install what you really need.
- Always install browser software from companies or places that you know. Software provided directly by Microsoft, Apple, Google, Adobe or Mozilla (the FireFox browser) can usually be trusted.
- If you want to install something but cannot be sure that it is trustworthy contact the ISS Service Desk or your IT Department before you install it.
- If your browser slows down considerably or your homepage changes unexpectedly or you get unwanted pop-ups, etc, report the problem immediately.
- Do not install any browser software that is provided via a website pop-up or potentially malicious email.

5. Protection from Common Internet Threats

A large and active criminal set of Internet users will try to get us to share valuable information with them, - information that will allow them to steal our identity or that of others. Whilst we can rely on ISS to inform us how we can protect ourselves, we also must be vigilant.

Threats change from time to time so we must keep up-to-date with current threats. ISS publish information on current threats[9]

> **Never answer email requests for your password. Do not respond to any email request for your password even if the requesting email appears to come from ISS, elsewhere in the University, your Bank, or anyone else—even if you know them.**

It is very straightforward for someone to make it seem as if an email is coming from someone it is not.

[9] http://www.lancs.ac.uk/iss/security/threatwatch/

6. Use of Cloud Services

More and more services are offered through 'the cloud', with data, irrespective of its classification or value, being stored on the Internet. Personal email services such as Hotmail (now Outlook.cm) or GMail have grown in popularity, as have data storage services, such as DropBox, SkyDrive, Google Docs and iCloud.

The services and how they manage the data they process is however, by their very nature, outside the control of the University. Unless the University has a contract with the service provider (as is the case with Live@Edu), this presents a significant risk in terms of being able to prevent a breach of the Data Protection Act (DPA). The DPA requires us to protect any personal[10] information we use within our day to day business, whether it be information or data about staff, students, customers or University contacts.

The section below therefore sets out the University's policy on the use of Cloud Services for the processing of personal data.

Further guidance on the appropriate use of Cloud Services and those that have been approved by the University is given at http://www.lancs.ac.uk/iss/security/Cloud_Computing_Service_Audit

Information that the University categorises as Personal data must not be processed on ad hoc Cloud Services[11].

Any information that falls into the Restricted category must be encrypted before being processed using a Cloud Service.

It is your responsibility to ensure that where systems can synchronise data automatically with Cloud Service storage *(such as DropBox or EverNote),* they must be configured in such a way as to prevent any Personal data from being automatically synchronised.

Do not use your University account (usernames or passwords) to access ad hoc Cloud Services

If your account for a cloud service becomes compromised (e.g. if you think others may have access to it, or your service provider announces that passwords have been accessed by a third party) and you have used that service to process any University data (personal or otherwise) you must report this to your Head of Department/Section and to ISS to ensure that appropriate steps may be taken to minimise its impact.

[10] The DPA defines 'Personal' data as data which relate to a living individual who can be identified either from that data itself or from a combination of that data and other information which is in the possession of, or is likely to come into the possession of, those in control of the data. Further guidance is outlined in the University's **Policy on Categorising and Protecting University Assets** (http://www.lancs.ac.uk/depts/recman/docs/SEC-2011-4-0009-Policy-on-Categorising-and-Protecting-University-Information-Assets.docx)

[11] In certain circumstances, Personal Data may be kept on Cloud Services for which the University has an agreement with the service provider (e.g. Live@Edu). It is however recommended that even in these circumstances, personal data should be encrypted where praticable

7. Use of Social Networking Tools

Use of social networks (e.g. LinkedIn, Facebook, Twitter) has become a valuable tool for staff and students alike and provides a quick and easy mechanism for collaborating with groups of people outside the University. It is however important when using any online collaboration service to avoid giving information which could inadvertently provide unauthorised access to personal or restricted data and to follow the mandatory guidance:

Do not re-use your University email address, username and password as your login to social networking sites.

Do not use personal accounts for work purposes - use your University email address for work-related correspondence.

Never share any restricted information or personal data (such as personal details of students or staff) on social networks.

Any information submitted to social media sites should be regarded as being published information (and remember that once published by you it can often quickly be republished by others).

If someone requests to network with you (e.g. as a friend on Facebook or connect with you via LinkedIn), it is strongly advised that you check that they sent the request before accepting it. Be aware that it is possible the request came from a 'fake' account (looking like the real person) designed to extract information from you.

Be wary of sharing your own personal information (such as your date of birth, address etc.) with others (this is especially common on Facebook, but how well do you know all those you have accepted as being your "friends"?).

Be aware of (and do not respond to) posts that are phishing for personal information

If you are a member of staff, you must not require that students become your "friends" in order to work collaboratively.[12]

Make sure you know the source of any information you are sharing with others (did that post you received and just shared with all your friends contain any copyrighted data?).

Be aware of the security controls and privacy setting within any social network service you use. The terms and conditions of such services mean that these can often be changed with little warning.

[12] This may give you access to personal data. Alternatives available are to set up a group (which does not require you to be their friend) or to use the University VLE for collaboration with student groups.

8. Basic Computer Safety

Always lock your computer screen when you leave your desk; it's not because we don't trust our colleagues, simply because we never quite know how long we'll be away, and it's the safest thing to do.
On windows: <Ctrl><Alt><Del> then <Alt>k (or <WindowsKey>L)

Always remember to log-off computers in public areas, such as meeting or training rooms, after you have used them.

If you ever suspect that your computer has been tampered with or compromised, you must inform ISS and receive their help.

The following points are likely to indicate something to worry about with computer hygiene:

- The computer or particular applications run slower than they used to.
- You're presented with additional requests to authenticate.
- You see unusual error messages in places where messages did not previously appear.
- You see popups claiming anti-virus software is out of date even if the installed version is current.

If in doubt, contact the ISS Service Desk.

Keeping your computer healthy:

- Set Windows Update to automatically download and install updates.
- Connect to a network often to allow Windows Update to run, and do not defer installing updates.
- Install updates for software when needed. Most, but not all, now warn when updates are needed.
- Only install software from sites you trust, whether to your computer or mobile device.
- Avoid running with administrator rights for longer than necessary.
- Always find out why you need to put in your password when asked by the computer. If in doubt, don't.

9. Disposal of Media

No media should be released for disposal if it contains data that is Restricted or Personal, or data that has not been classified (and may therefore include Restricted or Personal data).

Before a data storage device goes out of the control of the University, we must ensure that it contains no readable data. When a storage device is disposed of, it may contain data that could be recovered by someone else - merely deleting the file (or even reformatting the data volume) is not sufficient to make the data unrecoverable, since specialised software can be used to "undelete" a file or "unformat" a device to gain access to the data.

It is very important that the data left on old storage devices is not ignored, since the discovery of data that was not supposed to be published could damage the reputation of the University, or could leave the University in breach of contractual agreements or data protection legislation.

The kinds of data storage devices include:

- Printed material
- CDROMs
- Backup tapes, audio tapes, video tapes
- USB sticks
- Digital camera storage cards
- Hard Disk Drives
- Laptop and desktop computers normally contain a hard disk drive, so they also count unless is has been removed.

Properly ensuring that there is no recoverable data on media is particularly important with devices that have been used to store data that is classed as Restricted or Personal, since recovery of such data by a third party could have serious reputational or legal consequences.

If you're unsure whether or not a particular device may have contained Restricted or Personal data at some point you should assume that it has. The most reliable method of ensuring that the data on a device is unrecoverable is to make it the device permanently unusable. Doing this safely and effectively requires the right methods and equipment, and depends on the nature of the device:

- Printed material can be shredded (avoid "strip cut" shredders, use "cross cut", "diamond" or "confetti" shredders)
- Some paper shredders will also work on small numbers of CDROMs
- For Hard Disk Drives and Backup Tapes it is best to use a computer disposal company that offers secure media disposal. If the device does not contain (and has never contained) Restricted or Personal data, it may be more appropriate to securely erase the data on the drive.
- If you are unsure, contact the ISS Service Desk.

10. Information Security and Systems Development

Development and test systems and data must be kept separate when working with restricted data; live data must not be used for testing or development.

Software development for the purposes of research must fall under either the governance of the Information Security Policy and Processes or the research ethics guidelines.

When working with restricted data that is not covered by the research ethics guidelines, in-house development of applications must have a phase in the design process that requires ISS approval, in order that it meets their development standards.

Standards for development shall include specific measures to maintain application security to prevent malicious attacks, with programmers ensuring that the code is defended against (for example):

- SQL injection attacks
- Cross site scripting attacks
- Buffer over-runs

As part of the development standards, programmers will go through a security threat review with ISS staff to ensure that the information held in the system under development can be properly secured.

11. Legal framework and privacy

The University's Information Security Policy and Processes will be kept in-line with the current legal framework, and updated as necessary. The legal framework that applies to information security and privacy is made up of the legislation enumerated in the 'Relevant Law' section above. If there are any apparent contradictions between the University's Information Security documentation and that legal framework, the latter takes precedence. Such apparent conflicts should be raised, so that we can ensure the clarity of the institution's policy and processes.

Glossary

Term	Definition
3G Device	A device that accesses the internet through the mobile phone network. 3G devices include: smart phones such as iPhones and tablet devices such as iPads.
Access Control List (ACL)	An Access Control List is a list of the people or groups of people who are allowed to read or write a file or folder on a computer. On shared computers, like the servers which hold our H: drives, ACLs are used to ensure that only those people who should have access to files, do have access to those files.
Browser	Browser is the generic term for a software application that allows you to browse the internet. Examples are: Internet Explorer, Firefox, Chrome and Safari.
Buffer Overrun	A buffer overrun is a mechanism by which a malicious user of a program can take over or replace a vulnerable program through its user interface. Ensuring that a program is not vulnerable to such an attack is part of the role of the software developer and ISS.
Cross-site scripting	Cross-site scripting is a means by which a malicious user can access sensitive information entered in good faith by a web page user. Ensuring that a web site is not vulnerable to such an attack is part of the role of the software developer and ISS.
Encryption	Encryption is a process of scrambling the contents of a file (like a word document, or an excel spreadsheet) so that it cannot be read without being unscrambled (decrypted). When a file is encrypted, it is scrambled using a password which must be provided in order for it to be decrypted. If the password is kept secret, encrypting a file is a good way of protecting its contents.
Keylogger	A keylogger is hardware or software which is used—usually maliciously, to make a record of every keystroke on a keyboard. In the wrong hands, that can mean that the wrong people can get your password. Public-use PCs may be susceptible to having keyloggers installed.
Mobile Device	More generic than a 3G device (see above) a Mobile Device is a phone, tablet or laptop which can access the internet through Wifi or 3G networks.
Public Access PCs	Computers that are used by many different people, usually made available for use in public areas. You should be careful not to let a

	public access PC store your password, as it might then become available to the next person who uses the computer.
The Cloud	Companies offer various services which can be accessed through smart phones and 3G devices as well as computers; what they have in common is that the service is accessed through the internet, and all the data associated with the service is kept on servers somewhere on the internet. Examples of cloud-based services are: Hotmail, Gmail, Google Docs, Evernote, Dropbox and iCloud.
SQL Injection Attack	If the web interface to a database is not properly protected, a SQL injection attack allows a malicious user to access data in that database to which though ought not have access. Ensuring that a database is not vulnerable to such an attack is part of the role of the software developer and ISS.
Trojan	Unlike a virus, a Trojan is a program which, though it has a purported purpose, also has malicious intent. It is important that you trust the source of any software which you install on your computer, to ensure that you do not mistakenly install a Trojan. If you have any concerns, please call ISS.
USB Stick	A device which plugs into your computer and contains memory; it allows files to be copied into its memory so that the file can be transferred from one computer to another. They are also known as flash drives, and USB drives.
Virus	A computer virus is a program written with malicious intent which may be downloaded and installed by a user unintentionally. Protection against viruses is best handled through anti-virus software, available through ISS. Viruses are written for, and infect Windows PCs, Macs and other computers.
VPN	Virtual Private Network: using a virtual private network is a way of keeping data safe as it travels between computers. We restrict access to some systems at the university by requiring the use of a virtual private network to access them from off-campus.
WiFi	A wireless network. An example wireless network here, is “eduroam.”