IT Policies and Procedures 2025/28

APPROVED BY (SELT) ON (December 2025)

Applies to:	
Harrogate College	X
Keighley College	X
Leeds City College	X
Leeds Conservatoire	X
Leeds Sixth Form College / Pudsey Sixth Form College	X
Luminate Group Services	X
University Centre	X

CHANGE CONTROL

Version:	4.0	
Approval route		
Approval committee (ELT, SELT, Board)	**Date approved**	**Version**
SELT	December 2025	4.1
Name of author:	Graham Eland	
Name of responsible committee:	SELT	
Related policies: (list)	Data Protection Policy	
Equality impact assessment completed	**Date:**	
	Assessment type ☐ **Full** **X Part** ☐ **Not required**	
Environmental Impact Assessment Completed	**Date:**	
	☐ **Yes** ☐ **No** **X Not required**	
Policy will be communicated via:	Staff Intranet, Colleges websites	
Next review date:	September 2028	

Contents

Contents

1. OBJECTIVES AND DESIGN OVERVIEW

The purpose of this document is to define a common set of IT policies and guidance appropriate for use throughout the merged Luminate Education Group. The policies below will not be provided in this (single document) format, but served as multiple small / discrete pages on a policy portal hosted by the College.
Each section below will represent a separate (linked) page on the policy portal.

The policies and guidance take the best and most appropriate policy statements from the three legacy colleges, and combine these with a good practice IT policy framework provided by ISO: 27001 (formerly ISO:17799, the International Standards Organisations guidance on IT security). We have also aligned policies to good practice within the Further Education sector, to ensure that the resulting statements are aligned with the level of control and risk acceptable for the College.

We have selected a design where each policy complies with the following structure / rules:

- **Readability**: The policies are written in plain English, and in short sentences. No policy is longer than a page. All policies have been written in the second-person, to personalise them;
- **Brevity**: Where details or further examples are required / available, we use hyperlinks to another page;
- **Structure** - All policies have:
    a. A title;
    b. If applicable, a reference to ISO27001 (in square brackets);
    c. A paragraph on the principle/reason underlying the policy and the risk/implication of non-compliance;
    d. Paragraphs on the policy itself, including reference (hyperlinked) to definitions and linked content;
    e. A description of the type of policy compliance and who it is applicable to.

The ITSS departmental page on the College Information Portal will be the home page for all policies.

This framework is split into six main sections, Govern, Build, Operate, Manage, Secure and Respond.

FAQs

This shows the main structure of policies to go on the website:

Governance
Use of Policy, standards and guidance
Framework
Compliance with the Luminate Education Group IT Policy Framework
Mandatory, expected and advisory
Personnel Practices
Security Awareness Training

Secure
User id and Password Policy
Independent review of Information Security
Third Party Security

Computer Security
Network Connection
Encryption of hardware and software
User Access
Access to Systems Software and Utilities
Emergency Procedures/Privileged user ids

Build
Change Control

Operate
Backup and Recovery Policy
Operating Procedures
Contingency Plan
Software Patch Management
Capacity Planning
Computer Virus Control

Manage
Ownership and management of our resources and information
Data Protection Act and General Data Protection Regulation
Freedom of Information Act
Resource Classification
Resource Security
Hardware and Software Management

Respond
IT Service Desk

2. GOVERNANCE

Use of Policy, Standards and Guidance [1.1]

Without policies, standards and guidance included here, there is an increased risk of unauthorised access, loss of privacy, inappropriate changes, misuse and damage to our ITsystems.

To ensure that access to and the use of IT systems is appropriate, consistent and authorised, you must adhere to the IT Policy Framework.

We have rated each policy statement as mandatory, expected or advisory, which describes the level of compliance we expect.

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Framework

We have setup the IT Policy Framework to make it easy for you to access the policies and guidance that are appropriate to you. Click on the hyperlinks within each policy to access linked policies and guidance.

We will review the framework regularly and if there are any significant changes, we will post these on the College's Intranet.

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Compliance with the Luminate Education Group IT Policy Framework [1.3]

It is in all our interests to maintain security over our information and IT assets. You have a responsibility to support this, by protecting the security of your own data/information, and to not try to access other people's personal systems or information.

You will be held accountable for non-compliance with these polices and procedures, and for attempts to access systems or information that you are not entitled to (i.e. hacking).

To ensure Luminate Education Group staff, students and contractual staff are aware of their responsibilities over misuse of IT, policies have been drawn up that outline the consequences of such misuse (computer use, illegal or harmful use, email use, and hacking)

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

What is mandatory, expected and advisory?
We have used three headings to describe the policies importance, and therefore the level of notice you need to take and the consequences of ignoring them:

Mandatory
This is important to us, and you must comply with the policy

Expected
This outlines how we would like you to do something, and is provided to create an approach that is best for the whole College. We will not actively track compliance.

Advisory / Guidance
This is good practice, and should help you in defining appropriate actions.

We use your user id to track system activity in audit trails. This makes all actions performed on College systems attributable to an individual user. Where actions are inappropriate (e.g.hacking), the IT department will be alerted to this and investigate it (together with HR and Student Services).

The acceptable uses of IT resources is contained in this policy (computer use, illegal or harmful use, email use, and hacking)

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Human Resource Practices [4.1]
Our IT systems are for the use of staff and students as part of work and study. You should make use of them for these purposes, and in such a way that will not damage the reputation or the resources of the College.

You are also allowed to use the systems for some non-work/study activities, as long as these lay within the limits of acceptable use of IT systems and data. Reasonable use includes personal communications (eg emails) and Internet use, as long as these do not disrupt the work/study of others, threaten the reputation of the College or takes a disproportionate amount of time.

We use web filtering and anti-spam services to reduce the amount of unwanted email, however on occasions this has been known to block legitimate emails. If you are aware of an email that has been sent but blocked, contact the IT Service Desk, who may be able to release it.

We conduct regular audits to make sure that everyone understands what their responsibilities are and are complying with them.

The College has the right to perform periodic, random audits on email usage, Internet usage and file storage. We have implemented filtering services to safeguard inappropriate access to content and ensure appropriate use of our network resources. If we identify any illegal activity(for example under the Child Protection Act or Terrorism Act) you will be referred to the police for investigation.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Computer use - what are my responsibilities?
To ensure clarity of what we (and the law) feel is the appropriate use of our IT systems, we have set out the boundaries and definitions below.

Responsibilities
You have responsibility to protect the integrity and security of our systems and data; You should only access systems and data that are needed for your work. IT security controls should prevent you from accessing inappropriate systems / information, however, if these have not been appropriately set up, you should not attempt to
exploit the weaknesses;
If you are aware someone else is abusing the systems, you have a duty to inform a member of the IT department /management;

JANET is the academic network which links us with other Colleges/Universities and the Internet. We all work under the JANET acceptable use policy, and the College is bound by its rules.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

What is illegal or harmful use?

You may only access and use our website and network (including email) for lawful purposes. You are personally responsible for any transmission you send, post, access, or store via our network, including the content of any communication.

The following provides examples of illegal or harmful actions that are not permitted:

- **Copying/stealing:** Copying/stealing of material already written by another person or material protected by copyright, trademark, patent or other intellectual property rights;
- **Offensive Materials:** Distributing or posting material that is unlawful, libellous, defamatory, obscene, indecent, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory or otherwise objectionable. You may not access or use our website or network in any manner to send or distribute any images containing pornography;
- **Fraudulent Conduct:** Offering or distributing fraudulent goods, services, schemes, or promotions (e.g. make-money-fast schemes, chain letters, and

pyramid schemes);

- **Failure to Abide by Third-Party Website Policies:** Violating the rules, regulations, or policies that apply to any third-party network, server, computer database, or website that you access;
- **Harmful Content:** Distributing or posting harmful content including viruses, Trojan horses, worms, time bombs, zombies, cancel bots or any other computer programming routines that may damage, interfere with, secretly intercept or seize any system, program, data or personal information.

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How should I use electronic communications and e-mails?

You may not distribute, publish, or send through our network:

- unsolicited advertisements, solicitations, commercial e-mail messages or promotional messages of any kind (known as "spam");
- chain mail;
- numerous copies of the same or very similar messages;
- very large messages or files that disrupt a server, account, newsgroup, or chat service.

Likewise, you may not:

- participate in collecting e-mail addresses, screen names, or other identifiers of others without Luminate Education Group's prior written consent, a practice sometimes known as spidering or harvesting;
- participate in using software (including "spyware") designed to help spidering or harvesting;
- collect responses from unsolicited messages;
- use any of our mail servers or another site's mail server to relay mail without the permission of the Head of ITSS.
- Participate in e-mail bombing, i.e. flooding someone with numerous or large e-mail messages in an attempt to disrupt them, their or our site.

Your email mailbox is unlimited for emails and attachments (including all folders such as inbox and sent items).

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

What is hacking or disruptive activity?
You must not abuse the security of our website or network in any way. Examples include:

Hacking: Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security without the prior authorisation of the owner of the system or network;

Interception: Unauthorised monitoring of data or traffic (e.g. sniffing or key logging) on any network or system without the prior authorisation of the owner of the system or network;

Intentional Interference: Interference with service to any user, host or network including, denial-of-service attacks, mail bombing, news bombing, other flooding techniques, deliberate attempts to overload a system, and broadcast attacks;

Avoiding System Restrictions: Using manual or electronic means to avoid any limitations established by Luminate Education Group or attempting to gain unauthorised access to, alter, or destroy any information that relates to any Luminate Education Group or other end-user.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Security Awareness Training [4.5]

To help make sure everyone is aware of our security risk and requirements we have d an online computer security awareness training programme for all employees.

You will also receive periodic communications when we have made changes to the IT policies or when there are new legal requirements that you need to be aware of.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

What computer security awareness training do I need to be awareof?
As part of the new staff induction process, you should view online the computer security awareness programmes, so that you understand the potential threats to Luminate Education Group IT systems and your systems security responsibilities.

This training should be viewed online soon after joining the College (in line with College induction policy) and sessions will include:
(For all staff):
Personnel security and Acceptable uses of systems;
Disciplinary action of non compliance with these policies;
User id and password policy;
Security policy;
System access control;
Computer virus control and web filtering;
Forward planning (eg requesting new equipment or IT changes).(For advanced users, such as IT, MIS and e-learning staff):
Hardware and software (asset) management;Computer security;
Workstation security;
Backup and recovery;
Operating procedures;
Physical network connections;
Management of encryption for hardware/software;
Access to systems software and utilities;
Emergency procedures/privileged users;

Contingency plans;
Patch management;
Capacity and availability planning.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

3. SECURITY

User id and Password Policy [1.2]

To protect our computer systems and data from unauthorised or inappropriate access, everyone has been given an individual user id and password. This allows you access to the things you are entitled to access, and denies you access to the things you shouldn't.
You will be held liable for (inappropriate) actions taken using your user id, so you are responsible for setting a good password (that can't be guessed) and for not sharing it with anyone else.
Do not write your password down or disclosed it to anyone under any circumstances.

If you believe someone else knows your password, change it immediately. If you suspect they have used your user id to access the system, inform the IT department.
You are allowed three access attempts before being locked out of the system. You will need to contact IT to reset your account.

You should log out of whichever PC you are using when you have finished, or when you leave it unattended, to stop someone else using your user id.

If you leave the College we will suspend your user account and password and archive all files and emails. The College has the right to re-use your email address, and may access the files / emails if necessary.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

What are good passwords?

Passwords are for your safety, and to ensure the safety of your information.

The guidance below represents the minimum password quality standards you should apply. The underlined sections represent the controls that are enforced by the system.

If you are a **student**, with access to email, the Internet and coursework only, this would be: Minimum 6 characters;
Not a common / dictionary word or name.

If you are **College teaching or administration staff**, with access to core finance or student administration systems, this would be:
Minim• um 12 characters;
Contai•ning mixed alpha and numeric chars Not a common / dictionary word or name;
Changed every 180 days and not the same as one used in the last 12 months.

If you are **IT staff or application administrators (e.g. for the finance or MIS applications)**,with systems administration access rights, this would be:
Minim• um 8 characters;
Contai•ning mixed alpha and numeric characters or, Symbols found on your keyboard, such as blank spaces, or ! * - () : | / ?;

Does not contain three or more characters from your account name; Not a common / dictionary word or name;
Changed every 180 days and not the same as one used in the last 12 months.

Examples of bad passwords include personal information, such as your username, name, nickname, pet's name, places, address, birthday or hobbies.
Using a dictionary attack, a
hacker can guess an unchanged 'normal' dictionary word, common name (eg Dave or Leeds) or set of repeating characters (eg aaaaa) in around 2 minutes.
Examples of good passwords include words that are easy to remember, but with letters substituted for characters or numbers and using upper and lower case characters. For example:
H*P@ptmZ (where you remember hippopotamus)
rFRgr8Tr (where you remember refrigerator) Don't use these examples!

This document is classified as	Expected Policy, however elements of the policy will be enforced by system controls.				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Independent Review of Information Security [2.2]

To ensure that the security measures we have put in place to protect our IT resources are adequate, they are reviewed every 1-3 years.

This may be done by our External Auditors or by a third party who has the appropriate IT skills and experience to perform such an audit.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

Third Party Security [2.3]
From time to time we may use external staff (i.e. individuals that are not permanent employees of the College, such as temps, contractors or employees of a third party organisation) who will need access to our IT facilities as part of their work.

These third parties should be subject to the same policies as the rest of us, and need to be aware of their responsibilities over IT. If we don't ensure that they are aware of our policies and adhere to them, there is a greater risk of unauthorised or inappropriate access.

We do not allow third parties to access our systems without first making them aware of their responsibilities and our policies.

All third party user ids will have an agreed expiry date set. To avoid disruption, if your contract has been extended, please inform IT before the expected expiry date.

As a third party, you must comply with the College's policies.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

What are my responsibilities for third party access?
'Third part access' relates to allowing someone who is not permanently employed by the College (such as temps, contractors or employees of a third party organisation) to access a College system or use the College network (e.g. to access the Internet).

Responsibilities of College staff:
You must obtain permission from the Head of ITSS for any third party who is on site and needs to make use of IT facilities. You are not permitted to allow them to use their own laptop to log onto our network, but if required they can be given wireless access to the Internet;
The College will endeavour to provide IT equipment to third-parties where possible. Please request this via the IT Service Desk;
You must report any inappropriate activity that you become aware of to both the third party's reporting manager and to the Head of ITSS.

Responsibilities of the Head of ITSS:
You should investigate any access violation attempts involving the third party;
You should ensure all third party users accessing the College's IT environment do so with a user id and password that can be attributable to them;
You should ensure all third party access is time-bound (ie is one-time only, needs re-requesting regularly, or has a specific end date applied);
You should conduct periodic user access audit to ensure that no third party still has access to the College's systems or network once their contract has finished.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

Computer Security [6.1, 6.2, 6.3]
Computers are valuable, and can be damaged easily if not appropriately looked after. There are many environmental threats such as theft, but also excessive heat, water, etc. To protectour systems and software against theft and damage we need to set basic standards for the physical environments they are stored in.

- Key systems, such as servers, need high security;
- Network hardware, such as 'local' network hubs, need moderate security;
- Desktop hardware, such as classroom PCS, printers and projectors, need basic security;
- Portable hardware, such as laptops and PDAs, need sensible precautions;
- For other IT assets, such as software master disks, we need secure storage.

We do not permit staff to remove personal data about your students from the College's systems because they would then be outside the College's security mechanisms and therefore at a greater risk of unauthorised access. This is necessary to enable us to comply with the College's Data Protection Act obligations.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How do we protect our key systems and control access?
The key systems to the College relate to application and database servers, significant elements of the infrastructure (such as the SAN) and core network hardware, such as primary switches and the firewall. Failure of these key systems would cause a significant disruption to the College's operation.

To minimise this threat, we need to ensure that all key systems are physically secured from accidental / malicious damage and not exposed to inappropriate access and environmentally damaging factors such as excessive heat, moisture, dirt, etc.

The table below shows the controls we require in all the College computer rooms (Server/Data Centres) that contain key systems:

Threat	Server room countermeasure	Primary room	N/W & secondary
Fire	Fire detection and alarm system	✓	X
	Smoke detectors	✓	✓
	Fire suppression system	Pref	X
	Portable fire extinguishers	✓	✓
	Maintenance and testing of the portable fire extinguishers, and the fire detection and suppression systems	✓	✓
Water/flood	Hardware on raised floors	Pref	X
	There is adequate drainage in the building	✓	✓
	Water pipes do not run directly over the computer hardware / room	✓	✓
Systems Failure	Air conditioning	✓	Pref
	Hazardous and combustible materials, as well as backup tapes, stored at a safe distance from the site.	✓	✓
	Use of Uninterruptable Power Supply	✓	✓
	Specification of systems to include redundant hardware (duplicate power supplies, RAID disks, etc)	✓	✓
Access Controls Theft/damage	Computer room is only accessible to staff who are authorised to enter (i.e. locked). Changing all six-digit entry codes periodically, whenever a member of staff leaves the network support team and whenever suspected of being security compromised	✓	✓
	If third parties need access, for maintenance or support, for example, supervise their visit.	✓	✓
	Marking all master keys 'DO NOT DUPLICATE'	✓	✓
	Frosted glass and bars on the windows to prevent unauthorised access	✓	Pref
	IP CCTV is installed/monitored in the computer room	✓	✓

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How do we protect our PCs, printers and projectors? [7.3]

To ensure we all have IT assets (PCs, Printers, projectors, etc) that is available and working properly, we need to protect our workstations (desktop PCs), printers and other assets (eg projectors, smart boards, etc) against theft and damage.

All classrooms containing IT assets must be locked when not in use;
All new workstations will be asset tagged. Do not remove or change the tags;
Treat the IT assets with respect – don't rest coffee cups on it or put it somewhere where it may get damaged, etc.

For staff:
Only IT staff are allowed to move IT assets from one location to another. You should contact IT if you need any IT assets to be moved;
You should report any suspicious activity to the Head of ITSS;
You should not store any restricted data on workstations accessible to students

For students:
You are not allowed to plug in your own laptop to the College's network. You must connect it wirelessly. Please ask for help from the IT department; You are not allowed to remove any College IT assets from the College premises; You should report any suspicious activity to your tutor;
You are not allowed to unplug any equipment such as mice or keyboards; Do not eat or drink (except water) when using our IT systems.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	

Network Connection

To make sure we can minimise the risks of virus attack and hacking, we only allow College owned (and managed) IT assets to connect to our network.

Do not try to connect your own IT equipment (eg laptops and PDAs) to our network, directly via the Local Area Network (LAN) ports.

Students may only access systems via the designated student PCs located in classrooms and shared areas.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How do we secure the network?
To make sure we can minimise the risks of virus attack and hacking, the security of the network is the responsibility of the Head of ITSS.

It is their responsibility to:

- Define the network perimeter(s), and the level of security required to prevent unauthorised access;
- Ensure that all network and server assets (such as LAN-Servers, bridges, routers, etc) are physically secured from unauthorised access;
- Ensure that remote access (eg via wireless) is not possible unless authorised (eg using wireless encryption);
- Authorise (new) connections to the network;
- Maintain network diagrams and keep records of assets configuration (eg routers);
- Ensure the network is segmented (eg using Vlans) to create separate networks;
- All access to the College domain is validated by a user id and password.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

How do I secure my laptop or PDA?
Once portable devices, such as laptops or, have been removed from the College grounds they are no longer protected by our on-site security controls, and hence cannot be considered to be 'secure'.

You are responsible for their security, and there are a number of things you must do to ensure we can minimise the risk of damage, theft of assets and theft of our information.
You must ensure you have set a good password;
Do not leave it unattended in public places, such as on trains or in cafes Only hold the minimum of information on it (unless it is encrypted); Do not leave it in your car (even locked in the boot);
Please return it to IT annually, to ensure it includes all patches and updates and has been defragmented to maintain performance.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

How do I secure my disks?
Backup media (eg tapes) and software distribution disks (CDs/DVDs and their accompanying serial numbers / activation keys) are valuable to the College, both in terms of the purchase cost, but also in risk of unauthorised access to data from backup tapes. To minimise the risks of loss (accidental or theft) or damage (eg scratches, exposure to magnetism or excessive heat), all media should be held by the IT department.

Data Backup
All backup media must be stored securely, either in a fire safe on the site that hold its corresponding system, or in an alternate (not joined) building.

Software master disks
All software media should be centrally stored securely (along with its serial number /activation key), to prevent theft;
Only the IT department can install software;
All master disks must be signed out.

Student/staff backup
You must ensure after any application has been installed, that the disk will be returned to the IT department;
If you install media free software (e.g. that has been downloaded from the Internet) you must evidence proof of purchase (e.g. ownership or license count) or that it is freeware.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	

Encryption of Hardware and Software [9.8]
The best method of securing data from unauthorised viewing is to encrypt it. This means that, even if it is on a memory stick that is lost, the 'finder' cannot see it.

We use encryption in two places:

- The College wireless (Wi-Fi) is for the use of College-owned hardware (and some staff-owned hardware). All connections will be encrypted using WPA2 standards;
- If you are taking data off-site, which can be considered as restricted or private /confidential you must:

Consider if it is really necessary to remove it from site;
Encrypt it on the memory stick /disk.
Only unrestricted data (ie with no consequence for unauthorised viewing) can be stored on unencrypted memory sticks.

Note: If you forget the encryption password we cannot help you recover it. Your data will be lost, so ensure it is also backed up, such as to your personal network drive.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How do I encrypt my memory stick?
Data on a memory stick is normally unencrypted, so anyone with physical access to the memory stick can access it (eg if you have lost it). The only way of protecting your data from access (other than not losing the memory stick) is by encrypting the data.

To prevent this you can do one of the following:
Buy a hardware encrypted memory stick (preferably AES 256 standard). These are usually around twice the price of normal (unencrypted) ones. This contains the software to protect your data;
Buy or download an encryption application. There are many commercially available, and some free ones, such as True Crypt. Follow the (Internet) download and install instructions.

Set a good password, that you will not forget – encrypted data with no password cannot be recovered by the College.

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Who is responsible for asset (hardware and software) security?
The Head of ITSS is responsible for making sure that all IT assets (hardware and software) is appropriately secured. These responsibilities cover College-owned IT assets only.

Their responsibilities include:

Hardware
Store all contingency and backup encryption devices in the computer room;
Ensure that the 'encryption-keys' are only held by IT staff.

Software
Make sure that the Wi-Fi network is security enabled by using an encryption network key to protect it;
Keep all encryption software (e.g., Wi-Fi encryption key, laptop encryption keys) confidential within IT.
Change the encryption keys on a regular basis. You should change the data encryption key at least quarterly and the key encryption key changed at least annually.

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

User Access [10.1, 10.2, 10.3]
The aim of the College is to support learning and teaching, so we need to make sure our IT systems are accessible and support information sharing. However, we also have a number of computer systems that contain financial and personal data that should not be freely accessible.

To support both the sharing and security prerequisites, we have segregated our network to create:

- An information sharing segment for use by students and staff for learning activities. This should contain unrestricted data only, and has no restrictions on file sharing;
- An administration segment for use by administration and teaching staff for College-management tasks. This should hold any data classified as restricted or private / confidential. Security controls over access to this segment are enhanced, and file sharing is restricted. We will monitor activity on this part of the network.

All requests for access to either segment have to be authorised by the system owner.

Where possible and appropriate we will set up a single sign on process, to reduce the number of passwords staff and students need to remember. (Eg College Intranet and Email)systems. However, where this is not appropriate or possible, each system must be set up as an 'island of information', with its own security controls to ensure users (including IT staff and third parties) are prevented from accessing inappropriate areas of the system. (Eg Finance and Personnel)

We also make sure that the level of access staff and students have is appropriate and that anyone who leaves the employment of College or their course, has their account suspended promptly.

All users must log on with their own user id and password.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How do I get access to the system?

For staff:

If you need to access the College's system, your manager must complete the New User Access form, which defines the systems you are given access to and why.

If your role changes, or you find you need access to another system, you must complete the same form.

For staff, this needs to be signed by the Resource Owner or line manager and should then begiven to IT to update the systems.

For students:

New students are identified automatically during the enrolment process. This creates a user id and password for you. As part of the induction process you will be told your user id and password (except at Park Lane Campus, where you will have to request your user id and password from the resource Learning Centre).

If you have forgotten your password, you will be required to identify yourself, either in person at the IT Service Desk (with your id badge or student card) or via a request from the Learning Resource Centre or your tutor.

This document is classified as	Guidance policy

It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How do we make sure access remains appropriate?
To ensure that the list of authorised systems users is correct, and all leavers have had their access revoked, we perform a number of checks that result in suspension of user accounts.

We receive lists of leavers from Personnel and the student record services which triggers a process whereby we disable the user ids.

Occasionally this process fails, so If you are aware of any student / staff member who has left the College, please inform HR/Student services, who will inform IT who can then secure the user id to prevent misuse.

We also regularly check who has accessed our systems recently, and any user id that has not been accessed in the last 6 months will be followed up with Personnel. If you are expecting to be away for over 3 months, or have just returned to find your user id does not work, please call the IT Service Desk.

This document is classified as	Advisory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

What do we do about access violations?
We have measures in place to prevent and detect anyone attempting to gain unauthorised access to our systems (ie hacking).

We reviews logs and on any attempted access and suspicious activity. This may include attempting to guess passwords or using more sophisticated methods such as using system scanning tools. These logs include capture of the user id used for the attempted access.

This policy should reinforce our advice about not sharing user ids or divulging passwords.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Don't run unauthorised software [10.7, 10.8]
We use powerful utilities to help operate, maintain and develop our systems. They often allow enhanced access and we therefore protect them against unauthorised or inappropriate access.

Only IT have access to, and use, system utilities as any unauthorised access may lead to the integrity of data being impaired or significant disruption to our systems.

Similarly, access to systems or web development software (eg MySQL and Moodle) is restricted to authorised users only. All systems and application software discs are held securely by IT.

We keep a log of all system utilities that may be used to alter information, data or software.

When we do access any sensitive system utility programs, we log the activity and review the audit trails generated. This is especially important if we use contractors who use system utilities.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

Emergency Procedures / Privileged user ids [10.9]
We specify the level of access required by all students and staff to access systems appropriate for their work or course.

There may be some instances however where we need enhanced access to systems to perform emergency work. To do this, we use privileges user ids (eg using the Administration and Backup Operator), and as these bypass normal access controls, the risk of inappropriate or unauthorised access is higher.

We make sure that any activities performed with privileged user ids during emergency situations are properly controlled and reviewed.

We only use high level privileged user ids in the event of emergency and only by IT staff.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

4. BUILD AND ASSET MAINTENANCE

We develop large enterprise web systems and databases, which we build in-house. All in- house developed systems remain the intellectual property of Luminate Education Group and cannot be sold or used elsewhere else without the College's prior approval.

Our core systems (eg Finance, Student Records, Personnel, Payroll) use established software packages, which are maintained by the third parties who own them.

Our PCs use standard build with standard images.

All of our IT assets are asset tagged.

To create or replace IT systems (buy or develop) we have an agreed process which includes:

- Capital bids
- System development / tailoring
- Testing
- Standard build Change control Training

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

Change Control [2.1, 5.3, 13]
When changes are made to systems, there is a risk that they may disrupt or damage the application because they have not been properly tested or have not been authorised.

Changes are necessary to our systems from time to time to enhance them or to correct bugs. To ensure these changes do not disrupt 'normal' operation of the systems, and to ensure they are appropriate and unauthorised, we have a change control process in place to:

- Log requests;
- Configure and develop systems;
- Test;
- Implement;
- Train staff and students.

We assess the change requests received, and use the below table to determine how therequest will be dealt with:

Change/project cycle	Small change <5 days <£1000	Medium change 5 to 30 days £1k to £20k	Large change > 30 days >£30k
Requests logged	X		
Business risk assessment	X	X	X
Business Case		X	X
Project Initiation Document (PID), risk register & project plan		X	X
Project Board			X
Formal Project management & reporting			X
Formal User Acceptance Testing		X	X
Formal program change control		X	X
Post implementation review		X	X
User training		X	X

The 'X' in the above table indicates where the element of the change/project cycle is required to be completed.

Once implemented the system is subject to the same security as all systems (e.g. passwords)

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How do we request / capture small change requests?

Change/project cycle	Small change <5 days <£1000	Medium change 5 to 30 days £1k to £20k	Large change > 30 days >£30k
Requests logged	X		

A small change request would include, for example, setting up a new user.

Requests for changes or enhancements to systems are conducted via a call to the IT Service Desk.

Note that students inform their tutor of any changes or problems who contact the IT Service Desk.

The Resource Owner and the Head of ITSS review all change requests and authorises those to be progressed base upon the type of request. The Head of ITSS keeps a log of all change requests.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

How do we perform business risk assessment?

Change/project cycle	Small change <5 days <£1000	Medium change 5 to 30 days £1k to £20k	Large change > 30 days >£30k
Business Impact Assessment	X	X	X

All changes should include a Business Impact Assessment. This will ensure that we apply the right amount of control – a change may be costly but quick, slow but inexpensive, or trivial but with significant consequences if it goes wrong.

Answer the following questions:

- Is the success of the change critical to the College or another project, or could failure potentially damaging our reputation?
- Are the costs and expected benefits material to the College's finances? Will the change affect more than 25% of our staff /students?
- Are we inexperienced in performing changes of this type, or is the Supplier inexperienced
- / unproven?
- Is the project technically complex?

If the answer to any of the above questions is 'yes', we need to manage the project in line with either the Medium or Large change categories. The Resource Owner and the Head of ITSS must review all business impact assessments requests and authorise go-ahead.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

How do we initiate medium and large changes?

Change/project cycle	Small change <5 days <£1000	Medium change 5 to 30 days £1k to £20k	Large change > 30 days >£30k
Business Case		X	X
Project Initiation Document (PID), risk register & project plan		X	X

Medium changes include upgrades to systems. A large development would be a project over30 days.

The key stages that we use to initiate a larger change or project are:

- Write a Business Case, justifying why we need to spend the money / time;
- For larger projects, write a Project initiation Document (PID), which goes into greater detail justifying why the College needs the new or changed system, and includes the benefits of implementing it.

The Resource Owner also liaises with the Head of ITSS to update our IT asset register when the change is introduced.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

How do we configure and develop systems?

Change/project cycle	Small change <5 days <£1000	Medium change 5 to 30 days £1k to £20k	Large change > 30 days >£30k
Project Board			X
Formal Project management & reporting			X
Formal program change control		X	X

We develop web applications of various sizes and complexity.

For core systems (eg Finance and LIS) we use packaged software. Where possible we should use core systems functionality, however, where this is not available / adequate (and can't be commissioned from the software house for a reasonable fee) we may supplement the functionality with in-house (web-based) development. This has to follow the above change control framework. We do not make changes to core packages. These must be done by the third parties responsible for those applications.

When the systems are developed or configured we have different approaches, depending on the nature of the systems affected:

Small applications
We only install patches for these applications and do not conduct any development work.

Databases
We use databases (such as Access, SQL and MySQL) and any changes we make must be signed off by the Resource Owner.

Large applications
These are critical applications to the College and changes must be done by the third parties responsible for them (in the first instance).
We use separate live and test environments;
No change to the application software is put live by the third party without prior agreement on specific updates and audit trailing of actions taken.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

How do we test software?

We test software before implementing it into the live system to make sure that it operates as it should do and doesn't adversely affect other parts of the system. To do this, we use a separate test environment so we can safely test any changes to systems without affecting the live system.

In practice, for our key packaged software will be mostly tested by the third party but we should also test it before it goes live. This is called User Acceptance Testing (UAT) and entails either IT or staff from the department that the system change relates to most to do the testing. This is because they know how the

system should work and are able to verify whether the changed system works correctly. For other, less key applications, we may not always conduct UAT before it is put live.

The testing required changes depending on the type of change. For example, a minor patch may not need extensive testing, whereas a big system change will need a lot of testing of the programs that make up that change as well as other programs in the system that it may be connected to.

When we are happy that the software works as it should we sign off the test scripts to show that we have done the testing and it works.

Large systems developments must undergo stress testing and interface testing before they are released.

This document is classified as	Mandatory policy if the change relates to a key application and Expected policy for other applications.				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

How do we implement new programs or changes?

Change/project cycle	Small change <5 days <£1000	Medium change 5 to 30 days £1k to £20k	Large change > 30 days >£30k
Project Board			X
Formal Project management & reporting			X
Formal program change control		X	X
Post implementation review		X	X

We will not implement changes to systems until you can evidence satisfactory testing and sign off.

Some changes may be very quick but others may need the system to be unavailable to users for a while, depending on the nature of the change. We therefore liaise with the users in various departments to find the best time to implement the changes to minimise disruption.

In case there are any problems with the new software, we take a backup of the system before we put the changed programs into the live or test environment.

We keep a close eye on the operation of the system after a change has been implemented, by monitoring system performance and conducting periodic testing to verify that it is working satisfactorily. We also conduct a formal Post Implementation Review for larger projects to ensure that the system delivered is what we wanted.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

How do we train users?

Change/project cycle	Small change <5 days <£1000	Medium change 5 to 30 days £1k to £20k	Large change > 30 days >£30k
User training		X	X

The amount of training we need to receive is dependent on the nature of the change. For example, a small patch would have no impact on how the system operates from a user's perspective. A major change may mean that the system works different to what we're used to. We need to fit the training therefore to how much of the system has changed.

We also need to consider who needs to be trained. The training should be given therefore to people who are directly affected by the system change.

Depending on the nature of the change, the training process may be large and involve:

Schedule of training
Who needs to be trained and when

Rooms/resources
We need to make every effort to ensure that we have sufficient rooms and systems available to train our staff.

Privileged users

We often use 'privileged user', that is people who have a greater knowledge of the new system and are available to provide help to people on the new system, and to conduct training.

We also make sure all staff and students are aware of the changes to systems and how to use them through awareness training

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

5. SYSTEMS OPERATIONS

Backup and Recovery Policy [8.2]
We rely extensively on our computer systems, the loss of which would disrupt both staff and students significantly. We therefore back up our systems software, applications and data on a regular basis and conduct tests to ensure that data can be successfully recovered in the event of losing part or all of the computing facilities.
These backups also form part of our contingency plan should our systems be damaged or lost.

Students

Remember that you are responsible for your own work and although the College's network is backed up, any of your data on memory sticks is not backed up and so if you lose your memory stick you will lose the data on it unless you have kept a separate backup (e.g. copy your work to the network).

You must ensure that you keep any data you need from the PCs as they are regularly re-imaged and therefore all data will be lost.

This policy is advisory for all Luminate Education Group students.

Staff
You are responsible for ensuring that any data you want backed up is stored on the network. If you use a laptop, data is automatically saved to the hard drive (C:). If the laptop is lost or stolen, you will lose the data, so you should copy it to the network to ensure that it will be backed up.

You should not backup/copy confidential data to memory sticks or CDs unless it is encrypted.

This policy is expected for all Luminate Education Group IT, academic and admin staff.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

What are my responsibilities over backups and data restore?

As Head of ITSS (or designate), your responsibilities are:

- Maintain a record of how frequently backups should be taken, noting that any changes to software will need additional backups before the change is implemented;
- Store backups in a secure location at least 200m away from the environment of the main systems (such as in a different building to the main servers). This is important because you need to able to get to the backups if you can't get access to the College;
- Maintain a backup cycle of daily, weekly and four-weekly backups.
- Specific systems will also have a monthly backup, with finance and HR systems' data being stored for a 7 year period. MIS data backups will be kept in line with the data retention strategy;
- Maintain a log of the contents of backups held in the remote storage location; Conduct backups before and after any major system changes (e.g. following a new release of the application or following changes to the main applications); Conduct checks on backups undertaken when they have been completed; Conduct regular exercises to restore the data from tapes to ensure that it can be done successfully;
- Ensure that access to the backups is restricted to those staff with a legitimate need;
- Ensure that disposal of backups follows the disposal policy

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

Operating Procedures [8.7]

If we don't have standard procedures for looking after our systems, we may not adequately look after them, which may result in loss or corruption of data and/or systems.

To ensure that we look after our computer systems adequately and consistently, we have standard operating procedures, and these are carried out by our IT department.

We are in the process or reviewing documentation for all aspects of IT, including:

- All key procedures;
- Training;
- Storage and the availability of information on sensitive systems/data (available to applicable staff only);

- Configuration of systems

All documentation is reviewed and updated every two years, or after a major system change or upgrade.

We have documented the following procedures:
Backup and restore;
Exchange email;
Internet management;
Learning resources and staff areas
Management console;
Network management;
Printer management;
Software distribution;
Software user guides;
User management;
Virus protection;
Workstation management;
Scanner management;
Software release notes/installation notes;
IT service management.

We keep these procedures in IT and treat them as formal documents, whereby any changes are only made once approved the Head of ITSS

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

Contingency Plan [11.2]

The loss of our computer systems would cause us significant disruption. We therefore have a backup and contingency plan for all of our key systems of how to deal with the different scenarios that may cause the loss or corruption of our systems and how to recover from them.

The Head of ITSS and Resource Owners have put this plan together and they keep it up to date, a copy of which is stored off-site.

The Resource Owners specify the recovery timescales.

The Business Continuity Plan (BCP) procedures surrounding recovery, staff involvement, emergency procedures, public relations, etc.

Disaster recovery (DR) covers the recovery of systems (IT, telecoms, etc), and key areas of the business (HR, IT, Communications, Estates/Property, etc).

We test our contingency plans annually and the results of this feed into updating the plan.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

What does the contingency plan contain?
It is the Head of ITSS' responsibility, along with the Resource Owners, to co-ordinate and maintain the plan. There are many aspects to the contingency plan, and we have included the most important elements here:

Purpose and scope
We need to make clear what the purpose and scope of the plan are. The plan also states what it does not intend to achieve and why.

Plan owner and maintenance
Who is responsible for putting the plan together and keeps it up to date.

Roles and Responsibilities of each Disaster Recovery (DR) team member
Who the designated people are, their contact details, and what their roles are in a disaster.

Business Impact Analysis (BIA)
This shows what the impact of various scenarios may be on our computer systems. Scenarios include, for example, the system being unavailable for a day, or a virus corrupting the system. We also bear in mind the classification of systems to establish how important they are in our contingency strategy. We have documented what the impact of these scenarios are to the College and the students.

Criteria to activate the plan
How we detect and declare a disaster, and how we notify relevant personnel of what they need to do next.

Procedures to implement the recovery strategy
These are the detailed procedures of what we do, depending on the situation, to recover all identified applications.

Vital information
We define the vital information sources we have and how they should be accessed. These may include: financial (e.g. payroll) details;
supplier details, legal documents (e.g. contracts, insurance policies, title deeds, etc.) other service documents (e.g. service level agreements).

Testing procedures
We conduct testing to verify that the system works satisfactorily and we have recovered the data accurately. Note that depending on the situation, we may not recover all the data immediately.

Regular tests
We test the contingency plan at least once a year and all issues arising from the test are documented and followed-up to make it more effective.

This document is classified as	Advisory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

Patch Management
If the software version we use is not the most up to date, there is an increased risk that an unauthorised user may be able to exploit weaknesses in the operating system, including vulnerabilities to virus attacks. We ensure that we are no more than one Service Pack behind the current version to protect our systems.

We install all security patches immediately and check other patches to assess whether they are required. If it is needed and if the patch represents a large change, where possible we test it before implementing it.

We use automatic links via the internet to our software suppliers' web sites, such as Microsoft for Windows software, to ensure we receive regular software updates. PCs will be updated using the central Windows update server. Updates/patches for servers must be validated first as they may not need to be upgraded immediately.

Updates to the Internet filtering services are applied daily.

We automatically update our antivirus definition files immediately on release.

We also conduct periodic checks to make sure we are receiving these updates correctly.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

Capacity Planning

Our systems have finite resources, such as network bandwidth, disk space and memory. Our demand for these grows over time, and, unchecked, may result in them not being able to operate effectively (i.e. they're too slow and keep crashing) and we may not be able to meet any future needs we have for them.

We maintain a regular programme of capacity planning to ensure we always have available resources and service is not impacted.

The Head of ITSS, and Network Team, is responsible for capacity planning, and as such: Monitors network performance daily on an ad-hoc basis to identify any problems during the day;
Records and monitor systems capacity and identify how capacity volumes fluctuate overtime. This helps create a trend over time so you are thus able to determine how future needs of the College can be met.

This document is classified as	Advisory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

Computer Virus Control

Computer viruses can cause significant disruption to our systems, and we have measures in place to ensure that we are protected against them.

We use McAfee virus guard and Symantec Anti-Virus software to protect against any viruses, and we receive automatic updates via the Internet daily. Anti-virus software is installed on all servers and workstations (including laptops).

The anti-virus software can only scan for known viruses, and so we update it regularly to ensure that it can identify and protect our systems against viruses.

Although we permit the use of memory sticks, we strongly recommend that staff and students regularly scan their memory sticks for viruses. The anti-virus software automatically scans the content of memory sticks when there are inserted.

We conduct automatic scans of all systems and data daily to check for viruses and do not allow users to bypass the scanning process. This includes scanning of email attachments and Internet downloads.

You should not use any unauthorised data or programs from outside the College (i.e. games, malicious code written on home PCs, etc).

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

What is good practice against viruses?
To help minimise the threat of viruses, you should only visit trusted sites and only download trusted software.

We have resident anti-virus software installed that is scheduled to run every day. File scans on servers are performed on a regular basis.

Everyone
If you download or copy data from another site and bring to the College on a memory stick, make sure you scan it for viruses
Contact the IT Service Desk if you suspect a virus
Do not disable the antivirus software on any College PC;

Think before opening attachments from sources you don't know. They may contain viruses.

For IT staff
Do not disable antivirus software on any College PC;
Do not change systems in a way that could threaten security, such as adding rules to the firewall;
Ensure all IT systems are patched to the appropriate level, and especially that security patches have been applied.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

What do I do if I suspect a virus?
There are many types of viruses (e.g. worms, trojan horses, most rootkits, spyware). They can be used to monitor your activity on websites, can result in the loss of all data from your computer or our systems becoming unusable.

As a result of a virus, the screen may go blank and/or the mouse/keyboard will not respond, the system may be slow, or it may keep on crashing.

Viruses may also take advantage of network services such as the World Wide Web, e-mail, Instant Messaging, and file sharing systems to spread.

If you suspect a virus attack you must:

a) Isolate the memory stick or disk that you think may have introduced the virus;
b) Do not use the suspected personal computer;
c) Call the IT Service Desk immediately on 0113 386 1999

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	✓

6. SYSTEMS MANAGEMENT

Ownership and management of our resources and information [3.1, 3.2, 8.5]
If we don't manage our IT resources properly, there is a risk that we may breach legislation, not protect our systems adequately or not ensure that our systems are appropriate for the College.

We have a large number of IT systems at the College. These 'resources' have been purchased/developed by a number of people over time, and have different values to the College.

To ensure we apply the right amount of (security) control over them, we have allocated each with Resource Owners and classified them according to risk/value/amount of control required

The resource owner is responsible for setting the amount of security required (ie the classification).

The classification sets the amount of security we (the IT department) have applied to the system / information.

The Head of ITSS is responsible for securing systems in line with the Resource Owner's requirements and data classification.
We store all media (e.g., disks, memory sticks) securely stored with IT at all times when not in use.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

What are the responsibilities of the Resource Owner?
As an allocated resource owner, you are responsible for setting the level of control required to provide appropriate confidentiality, integrity and availability of your resource. The IT department will configure controls to the requirements you have outlined.

Requirements include:
Defining what the information, software and / or hardware is needed for. For information, this means ensuring it is complete and accurate and that you have complied with the Data Protection Act and the Freedom of Information Act; Deciding how important the information, software or hardware is for the College(e.g. financial value or reputational damage if it is lost, damaged or distributed widely); Deciding how the information, software or hardware should be protected, and who should have access to it;

The Resource Owner is responsible for approving access to the information, software and /or hardware.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

Data Protection Act
The Data Protection Act (DPA) defines what is acceptable and not allowed in terms of data handling for the United Kingdom.

We must comply with the Act to ensure we are not prosecuted.

The Data Protection Act representative(s) are responsible for ensuring that we comply with the Act.

There are eight key principles of the Act that explain what data-handling means in practice: Data may only be used for the specific purposes for which it was collected;
Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information;

Individuals have a right of access to the information held about them; Personal information may be kept for no longer than is necessary and must be kept up to date;
Personal information may not be transmitted outside Europe unless the individual whom it is about has consented or adequate protection is in place;
Subject to some exceptions for organisations that only do very simple processing, and for domestic use, all entities that process personal information must register with the Information Commissioner's Office;
Entities holding personal information are required to have adequate security measures in place;
Subjects have the right to have factually incorrect information corrected.

This document is classified as	Mandatory policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

Freedom of Information Act
The Freedom of Information Act (FoI) underlies the right of people to know about public bodies, such as colleges. As well as the "general right of access", the Act places a duty on public authorities to adopt and maintain pro-active "publication schemes" for the routine release of important information (such as annual reports and accounts).

Any person or company can request information under the Act. There is no special format for a request. Applicants do not need to mention the act when making a request. Applicants do not have to give a reason for their request.

We have 20 working days to respond to these requests.

We can refuse a request for information if it costs more than £600, including time spent searching for files.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

Resource Classification [3.2]
A ‘resource’ is an IT system or piece of software / information that is of value to the College. To help us secure resources to an appropriate level (ie not too much security,
Preventing you from accessing the things you need to work, or too little, compromising the confidentiality, integrity or availability of the resource), we have defined four resource categories.

Restricted
Information and data is of the highest importance to the College as a whole, and loss of it might result in significant direct and indirect cost for replacement or reputational damage.

Examples of Restricted classification information may include Child Protection Act data.

Private or Confidential
Information and data is important to the College, and maintaining its confidentiality and integrity is an obligation under financial regulations, the Data Protection Act, Human Rights Act, etc.

Examples of Private or Confidential classification data may include: Financial data;
Personal information, such as HR records, qualifications, appraisals, etc;
Your own files and data (eg course work stored on your personal network drive).

Unrestricted
The information may be viewed by anyone internal or external to the College. It does not require any additional restriction apart from standard College information security requirements (eg preventing people from changing it).

Examples of Unrestricted data will include pages on the Intranet.

The level of security / control we allocate to the resource is aligned to these categories.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

Resource Security
To enable the IT department to configure appropriate levels of (security, backup and recovery) control over College Resources, the resource owner must define both the sensitivity of the information and its value/requirement for the resource.

We have created standard classifications for these, which encompass a set of controls over Access (to protect sensitive data) and Backup/Recovery (to protect valuable date). If your data requires additional controls, you must agree these with the Head of ITSS.

The IT department defines security and resilience controls aligned to the classifications as follows:

Classification	Access controls	Backup frequency	Disaster recovery priority
Restricted	• Access via the staff domain only. • Stored in separate secure network area on the College SAN (storage area network) with access restricted to specific named individuals or a small group only. • Administrator access restricted to the Backup id only, and we log all access. • Do not email restricted files or store them on your C:drive. • All documents should be password protected.	Daily full backup stored securely off-line. Replication of SAN snapshot 3 times daily	Recovery within 24 hours
Private or confidential	• Access via the staff domain only. • Stored in secure network area with access by authorised group membership only. • Remote access if deemed appropriate (in accordance With College policy).	Daily full backup stored securely off-line. Replication of SAN snapshot 3 times daily	Recovery within 24 hours

Unrestricted	• Unrestricted read access from any point on the College network. • Edit access restricted by group membership. • Remote access permitted where necessary		Recovery within 5 days

Within the constraints of each classification, the IT department has put in place sufficient controls to ensure the above level of security, backup and recovery is achievable.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

Hardware & Software Management [5.1, 5.2, 5.4, 5.5, 7.1, 8.1, 8.3, 8.4, 8.5]

Without properly maintained and secure systems, we won't be able to support students and operate effectively as a College.

The Head of IS Department is solely responsible for software and software purchasing.

We have a consistent approach to IT purchasing, we keep a log of all IT assets we have and make sure all systems are properly maintained. The College systems are the property of the college and cannot be removed from the college's premises.

Before purchasing any IT assets (even evaluation software), you should seek advice and permission from the Head of ITSS.

The Head of ITSS has overall responsible for making sure:

- The right systems are in place for our needs(purchasing),
- They are held securely to prevent unauthorised copying or theft, They work properly, and
- They are disposed of effectively.

We comply with the principles outlines by the Federation Against Software Theft (FAST), a not for profit organisation with the aim of eradicating Software theft in the UK.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

What are my responsibilities for IT asset (hardware and software) purchasing?

When there are requests for additional assets we check our own available assets first to see if there is any available.

Hardware and software are only to be purchased and installed by the IT department. This will ensure we always have standard specification systems (compatible with our existing systems) and, for software, proof of purchase (aligned to FAST guidelines). This will also enable us to benefit from any discounts from bulk buying.

As the Head of ITSS you are responsible for:

- Maintaining a list of all software and hardware suppliers; Maintaining a record of all software and hardware at the College;
- Ensuring we have licences and proof of purchase for all software;
- Getting the best possible price/discounts for software and hardware purchases; Ensuring that we buy software that is compatible with existing systems as far as possible;
- Ensuring maintenance agreements are in place.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

How do I keep track of our IT assets?
The Head of ITSS is responsible for the management of our IT assets. These responsibilities include:

Hardware
Ensuring that all IT hardware (workstations, printers, etc) are tagged with a unique identification number and have responsibility assigned for them; Maintaining a register of all devices;
Authorising the removal or transfer of hardware;
Informing contractors of their obligation to return any assets used during their contract and to ensure it has been returned before they leave;
Ensuring that regular audits are conducted of assets to ensure that our records remain up to date;

Software
Maintaining a software register of all software held; Maintaining sufficient licences for installed software; Ensuring that regular audits are conducted of software to ensure that our records remain up to date.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

What are my responsibilities over hardware maintenance?
We use maintenance contracts to ensure that our systems continue to operate effectively or are replaced in the event of failure.

The Head of ITSS is responsible for ensuring that appropriate Service Level Agreements (SLAs) are included in the terms of these contracts. These requirements should include the provision of replacement hardware if required.

Hardware support expectations are:

- All key servers are always on hardware support;
- PCs are on a 4 year replacement cycle, with hardware cover via the manufacturer for the full 4 to 5 years;
- Other hardware has support for the first three years, but then can continue in operation maintenance free.

The Head of ITSS will maintain a schedule to keep track on when hardware may be due to be replaced and to ensure that contracts do not lapse without knowledge.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

How do I safely dispose of IT assets (hardware and software)?
If we don't dispose of software appropriately, restricted data may be obtained by unauthorised people or software licensing agreements may be breached. We may also breach Health & Safety legislation or the Waste Electrical and Electronic Equipment (WEEE)directive.

The Head of ITSS is responsible for all the College's hardware and software disposal. We dispose of IT assets if they are obsolete, no longer working or no longer needed.

Hardware and software
For both hardware and software, you should request an update to the asset register and include reasons for the disposal;
We conduct regular audits of all software and hardware to check that we have accurate records of what we have and have disposed of.

For software & data:
Destroy the disk, erase software and data so it is in a non-readable format. This may involve incineration or shredding;
Remove all erasable software and data from storage devices (e.g. hard drives, memory sticks, disks etc) prior to disposal

For hardware:
Dispose of old, obsolete or damaged hardware in one of the following ways:
Transfer to another department (if it remains operational and of value);
Scrap it, bearing in mind the requirements for disposing of software beforehand;
Give it to an authorised body, which is WEEE compliant, to ensure that we comply with Health & Safety legislation.

The College cannot recycle PCs to be sold to staff / students or given to charity as the cost and resource associated with removing licensed software and data cannot be justified.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

What do we do about system incidents?
There may be instances where problems occur with our systems and if they were not attended to and resolved, there may be errors or systems may fail to work adequately.

We follow ITIL principles over incident management, where we aim to restore normal operations as soon as possible following an incident.

The key activities of incident management that we follow are:

Incident detection and recording
We operate a IT Service Desk to log all incidents reported to us.

Classification and initial support
We assess the significance of the incident based upon the impact that the incident is having on the staff or the students involved. Incidents are given a rating to help prioritise it amongst the other work that needs to be completed. Classifications used are:
Whole College outage;

Campus outage;
Classroom outage;
System down;
Over 20% of class / department affected;
Individual down;
Individual query.

Often the IT Service Desk can resolve an incident but if not, these incidents are referred to a member of the IT team (first and second line support).

The incident may be part of a known issue or will be resolved as part of an ongoing change request, in which case we log these details.

Investigation and diagnosis
We investigate the cause of the incident to help us to resolve it.

Resolution and recovery
The resolution of the incident (a fix of the problem or a temporary workaround until a proper fix can be found) is put in place.

Incident closure
Once the incident has been resolved, we tell (email)) the person who informed us of the incident and mark it as closed on the IT Service Desk.

Ownership, monitoring, tracking and communication.
Although closed, we keep an eye on the incident for a week after closure.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

What do we do about problems with systems?
Errors in our systems may cause disruption or, if unchecked, may lead to more serious problems. Like Incident management, we aim to maintain a Problem Management system to minimise the impact of any adverse impact of any errors within our systems.

A problem is often identified as a result of multiple incidents that show common symptoms. Problems can also be identified from a single significant Incident, for which the cause is unknown, but for which the impact is significant. Problems can be complex or require extended research to fix them, and are generally dealt with by second level IT support.

The main difference between problem and incident management is:
For problem management, we try to find the root cause of an error and resolve it to reduce the likelihood of the problem reoccurring;
For incident management, our primary priority is to provide an immediate work- around to fix the problem as quickly as possible, regardless of its underlying cause.

The key stages of problem management are:

Problem identification and recording
We operate a IT Service Desk to log all problems reported to us.

Problem classification
We assess the problem and classify it according to the impact on the College

Problem investigation and diagnosis.
We investigate the cause of the problem to help us to resolve it.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓				

IT Service Desk
Without an effective method of logging, monitoring and co-ordinating problems and incidents, we will find it more difficult to support you in an efficient and effective manner, while also maintaining our systems.

We use an IT Service Desk to manage, co-ordinate and resolve IT-related problems and incidents as soon as possible. This ensures that no request is lost, forgotten or ignored, and that support trends can be analysed to resolve the root causes of recurring problems.

In order to get the quickest response, the IT Service Desk should be your first point of contact. Do not call a specific member of the IT staff as they may not be available (and your support will be delayed).

For students and staff
The IT Service Desk contact details are as follows: 0113 386 1999

For IT
We have policies for the maintenance of the incidents and problems

As part of these processes, you must keep users informed of progress on their calls and aim to resolve them within reasonable timescales.

This document is classified as	Expected policy				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓	✓	

Resource classification
This form should be completed by the Resource Owner to assist in classification of assets. Information has three facets that need to be considered in its classification:

- **Confidentiality** – This considers the impact of allowing unauthorised individuals to view the data /information;
- **Integrity** – This considers how we can maintain the completeness and accuracy of the data / information;
- **Availability** – This considers when and where the data/ information should be availability, and after an incident, how quick it should be recovered.

Confidentiality	
Is personal data to be held?	Yes / No
Does the information come under the remit of the Data Protection Act?	Yes / No

Does the information include financial data that may require limited access?	Yes / No				
Integrity					
What is the consequence of information loss?	1 (Min)	2	3	4	5 (Max)
Reputational Damage					
Financial cost of loss and recovery					
Operational disruption					
Availability					
What would be the impact of downtime / unavailability of the information	1 (Min)	2	3	4	5 (Max)
1 hour					
4 hours					
1 day					
1 week					
1 month					
Indefinite loss					

Resulting asset classification (tick appropriate)	Restricted	Private / confidential	Unrestricted

Do you need additional controls beyond those defined within the standard asset classifications?	Yes / No

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

Business Impact Assessment

This form should be completed by the project sponsor to assist in selection of the best approach to project delivery and risk management.

For the proposed project	1 (Min)	2	3	4	5 (Max)
Is the success of the change critical to the College or another (key) project, or could failure potentially damaging our reputation?					
Are the costs and expected benefits material to the College's finances?					
Will the change affect a large percentage of the staff or student population?					
Are we inexperienced in performing changes of this type, or is the Supplier inexperienced / unproven?					
Is the project technically complex?					

If you record a score of 5 to 10, the project can be classified as 'small change' If you record a score of 6 to 20, the project can be classified as 'medium change' If you record a score over 20, the project must be classified as
'large change'

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		

Project Mandate

1. **[Project name]**

Version	Date	Author	Change
0.0			
0.1			

This document is a blank proforma, provided as guidance to enable a project sponsor / project manager to effectively communicate project requirements in a manner consistent with other College projects and general accepted good practice.

Project objectives

[Overview paragraph on the high level objectives of the project]

Project scope

[Description of the elements of the project that are in scope / to be included, and any specific scope exclusions]

Constraints

1. [The criteria that would be expected of the project, for example delivery dates, future cost savings. These will eventually be used to define the formal acceptancecriteria]
2. .
3.

Outline business case

[A description of the costs, benefits and requirements for the system / development /change]

Project tolerances

[Where there is flexibility, such as delivery date or phased implementation, list it here]

Interfaces

[Consider the impact this project / resulting system has on other projects or Collegesystems]

Project personnel

[List:

- The project sponsor (senior manager / exec/etc)
- The project manager
- The members of the projectboard
- Other key stakeholders

]

It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

Project Initiation Document

2. [Project name]

Version	Date	Author	Change
0.0			
0.1			

This document is a blank proforma, provided as guidance to enable a project sponsor / project manager to effectively communicate details of the project's requirements, approach to delivery, risks, resource requirements and delivery timetable, in a manner consistent with other College projects and general accepted good practice.

Business case

[A (more detailed) description of the costs, benefits and requirements for the system /development / change]

Defined project approach

[Describe how the project will deliver the solution]

Project brief

[Describe what the solution will include / look like / do. Each attribute should be classified (by importance)]

Functional attributes

No	Function	Classification	Weighting
1		Show Stopper	1.5
9		Important	1.0
10			

Generic attributes

No	Generic requirement	Classification	Weighting
41		Show stopper	1.5
42		Show stopper	1.5

Project management team

[List:

- The project sponsor (senior manager / exec/etc)

- The project manager
- The members of the projectboard
- Other key stakeholders

]

Project administration

[Describe how the project will be managed, for example describe the key documents, project board / team members, groups to be consulted with, etc]

Quality plan

[Outline how quality should affect development. Consider:

- Review of project documents
- How to get assurance on project deliverables (eg does software workcorrectly?)
- How to evidence to third party (eg auditors) that the solution is aligned to your requirements (and those of the College)

]

Project Tolerances and change control.

[Outline where the original requirements can be flexed on time, budget or quality, while still allowing the project to deliver an 'acceptable' solution.]

Project controls

[Outline how you intend to keep the project board / senior management appraised on the (successful) progress of the project]

Project files

[How are you going to manage the information and coordinate the project resources in an efficient and effective manner]

Implementation decision and contingency plan

[Define what are the key decision points in the project, and what will support a positive decision (eg system selection, acceptance testing, go-live]

Appendix A - Risk log

Risks impact / probability rated as 0 (none / never) to 3 (high / likely). Scores 0-6 rated as low, 7-12 rated as moderate and 13+ as high

Risk	Impact Financial	Impact Reputation	Impact People/ Other	Total Impact	Probability	Ranking	Risk	Controls
XXX [event] may occur, leading to YYY [consequence]	3	3	2	8	3	24	High	How you will prevent this from occurring, or fix it rapidly afterwards

Appendix B - Project plan

[Include a project plan or set of key milestones / dates]

This document is classified as	Guidance				
It is applicable to:	IT staff	Academic staff	Administration staff	Students	Contractors & guests
	✓	✓	✓		✓

Terms and Definitions

[To be included throughout the framework and 'alternate text'].
Not all references are currently cross-referenced to the text in the policies.
Additional linksto the words need including wherever they appear in the policies.

Term	Definition / text to include
Audit trail	Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.
Availability	Information is accessible and available when and where you need it. Backups, etc, are performed to ensure it isn't lost.
Assets / IT assets	Any IT equipment, software or data of value to the College. This includes hardware (physical equipment such as computers, projectors, PDAs, etc), software (operating systems, applications, tools / utilities) and data (files, documents and College-owned intellectual property, such as training material, music and video).
Backup	**Backup** is the making copies of data so that these additional copies may be used to restore the original after a data loss event.
Chain mail	Chain mail is the email equivalent of the **chain letter** that consists of a message that attempts to induce the recipient to make a number of copies of the letter and then pass them on to as many recipients as possible. These can be used to spread viruses or to clog up systems.
Change	The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.
Change Control	The procedure to ensure that all Changes are controlled, including the submission, analysis, decision making, approval, implementation and post implementation of the Change.
Change document	Request for Change, Change control form, Change order, Change record.
Change log	A log of Requests for Change raised during a project, showing information on each Change, its evaluation, what decisions have been made and its current status, e.g. raised, reviewed, approved, implemented, or closed.
Classification	Process of formally grouping items by type, e.g. software, hardware, documentation, environment, application.
Chat room	Any form of on-line communication.
Confidentiality	Information is only accessible to those authorised to see it.
Configuration	This is the choice of hardware, software, firmware, and documentation of the College. The configuration affects system function and performance.
Data	Data refers to information or facts usually collected as the result of experience, observation or experiment, or processes within a computer system, or premises. Data may consist of numbers, words, or images.
Database	A structured collection of records or data that is stored in a computer system.
Data Protection Act	The Data Protection Act 1998 (DPA) defines a legal basis for handling of information in the United Kingdom (UK) relating to people living within. It is the main piece of legislation that governs the protection of personal data in the UK. The Act defines eight data protection principles.
Disk	A general category of a computer storage, in which data is recorded on

Term	Definition / text to include
	round and rotating surfaces (eg CDs, DVDs)
Encryption	Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
Environment/live environment	A collection of hardware, software, network communications and procedures that work together to provide a discrete type of computer service. There may be one or more environments on a physical platform e.g. test, production. An environment has unique features and characteristics that dictate how they are administered in similar, yet diverse, manners. Live environment is the environment that is used for every day processing and is distinct from other environments such as Test environment.
Firewall	Hardware or software that tightly controls and manages the connections allowed to networks or information technology devices that it protects.
Gigabyte	**Gigabyte** is a multiple of the unit byte for digital information storage. A **byte** is a basic unit of measurement of information storage in computers.
Hacking	The practice of breaking into computers without permission.
Hardware	Hardware is a general term that refers to the physical artifacts of technology. It may also mean the physical components of a computer system, in the form of computer hardware.
Head of ITSS	Person with overall responsibility for the management of the IT department and resources in Luminate Education Group
IT Service Desk / Helpdesk	The IT Service Desk is an information and assistance resource that troubleshoots problems with computers or similar products
id/user id	This is the unique reference (identifier) for a user of a computer system.
Impact	Measure of the business criticality of an Incident.
Incident	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Information	Information is broadly classed as communication, data, instruction, and/or knowledge. Personal information is that which related to an individual.
Information security	Preservation of confidentiality, integrity and availability of information.
Integrity	Information is as accurate and complete as possible, and only appropriate users can make changes.
Internet	The Internet is a global network of interconnected computers, enabling users to share information along multiple channels.
ITIL	Information Technology Infrastructure Library is a set of concepts and policies for managing IT infrastructure, development and operations.
IT / ICT	Information technology (IT) is the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware. IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and securely retrieve information. ICT is Information & Communication Technology, such as network and telecoms.
IT Device	Any device involved with the processing, storage, or forwarding of

Term	Definition / text to include
	information making use of the Luminate Education Group infrastructure or attached to our network. These devices include, but are not limited to, laptop computers, desktop computers, personal digital assistants, servers, and network devices such as routers or switches, and printers.
IT Resources	The full set of information technology devices (personal computers, printers, servers, networking devices, etc.) involved in the processing, storage, and transmission of information.
Encryption Key	Piece of information that determines the functional output of a cryptographic algorithm or cipher
Known error	An Incident or Problem for which the root cause is known and for which a temporary Work-around or a permanent alternative has been identified.
Laptop	A **laptop** (also known as a **notebook**) is a personal computer designed for mobile use small enough to sit on one's lap
Log	Manual or electronic storage of data
Memory stick	A removable memory storage device.
MSN Messenger	Instant messaging service
Network	A network is a computer network covering a physical area. A small network is called a Local Area Network (LAN), like a home, office, or small group of buildings, such as a college. A larger network that covers a wider geographical area is a Wide Area Network (WAN)
Network hub and switch	A device for connecting multiple devices together and thus making them act as a single network.
Packaged software	Software application developed by a third party that is available to buy. The third party tends to retain the source code and only they can make changes to it.
Password	A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource
Peripheral	Device attached to a host computer whose primary functionality is dependent upon the host, and can therefore be considered as expanding the hosts capabilities, while not forming part of the system's core architecture
Personal Digital Assistant (PDA)	A handheld computer, also known as a palmtop computer
Policy	A policy is a deliberate plan of action to guide decisions and achieve rational outcome(s).
Policy Framework	A collection of policies to achieve objectives
Portal	A site that functions as a point of access to information on the Internet
Priority	Sequence in which an Incident or Problem needs to be resolved, based on impact and urgency.
Privileged user/ID	User account with enhanced access to systems in excess of 'normal' users.
Problem	Unknown underlying cause of one or more Incidents.
Process	A connected series of actions, activities, Changes etc. performed by agents with the intent of satisfying a purpose or achieving a goal.
Release	A collection of new and/or changes which are tested and introduced into the live environment together.
Role	A set of responsibilities, activities and authorisations.
Resources	A resource is an IT system or piece of software/information that is of value to the College

Term	Definition / text to include
Risk assessment	The likelihood and impact of problems / threats / vulnerabilities disrupting IT systems and service.
Risk management	The likelihood and impact of problems / threats / vulnerabilities disrupting IT systems and service AND the controls / actions management has put in place to mitigate these.
SAN	Storage Area Network - network designed to attach computer storage devices
Security	Protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
Server	A server application, operating system, computer, or appliance used to co-ordinate and manage services, such as email, printing, applications.
Service Level Agreement	A written agreement between a service provider and Customer(s) that documents agreed service levels for a service.
Software	Computer software, or just software is a general term used to describe a collection of computer programs, procedures and documentation that perform some tasks on a computer system.
Software environment	Software used to support the application, such as operating system, database management system, development tools, compilers, and application software.
Software licence	A legal instrument governing the usage or redistribution of copyright protected software.
Standard	A *standard practice* or procedure gives a set of instructions for performing operations or functions. For example, there are detailed standard operating procedures for operation of a nuclear power plant. A *standard guide* is general information or options which do not require a specific course of action.
Software developer	A software developer is a person or organization concerned with facets of the software development process wider than design and coding, a somewhat broader scope of computer programming or a specialty of project managing including some aspects of software product management.
Software patch	Software that is distributed to fix a specific set of problems or vulnerabilities in such things as computer programs or operating systems. A computer vendor will usually distribute a patch as a replacement for or an insertion in compiled code within computer operating systems or applications.
Software testing	Software Testing is an empirical investigation conducted to provide stakeholders with information about the quality of the product orservice under test, with respect to the context in which it is intended tooperate.
Spam	Unsolicited or undesired electronic messages
Spyware	Spyware is computer software that is installed surreptitiously on a personal computer to collect information about a user, their computer or browsing habits without the user's informed consent
System	An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective.
System software	Computer software that provides the infrastructure over which programs can operate, i.e. it manages and controls computer hardware so that

Term	Definition / text to include
	application software can perform.
Test script	A test script in software testing is a set of instructions that will be performed on the system under test to test that the system functions as expected. These steps can be executed manually or automatically.
User	Any individual who uses an information technology device such as a computer.
Utilities	System software is closely related to, but distinct from Operating System software.
Virus	A computer program that typically hides in the background and replicates itself from one information technology device to another by attaching itself to existing programs or parts of the operating system. A virus often automatically spreads to other information technology devices via the sharing of computer media, mail attachments, or website transfers.
Website	A website (or "web site") is a collection of related web pages, images, videos or other digital assets that are hosted on one web server, usually accessible via the Internet.
Wireless/Wi-Fi	Wi-Fi allows computers to connect o other devices without the need to wires, hence the term, 'wireless'. It is supported by most personal computer operating systems, many game consoles, laptops, smart phones, printers and other peripherals.
Workstation	A PC designed for technical or scientific applications. Intended primarily to be used by one person at a time, commonly connected to a local area network.