INFORMATION SECURITY POLICY
August 2018

SOUTH THAMES COLLEGES GROUP
KINGSTON HALL ROAD
KINGSTON
SURREY KT1 2AQ

Policy Title: Information Security Policy		Staff Member Responsible: Director of IT Services
Version: 2	Date EqIA Undertaken:	Review Date: July 2019

Table of Contents

1. Information Security Policy

Overview
Information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as the South Thames Colleges Group, where information will relate to learning, teaching, administration and management.

This policy is concerned with the management and security of the Colleges Group information assets; (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to the organisation) and the use made of these assets by its members and others who may legitimately process College information on behalf of the College.

Purpose
An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

Scope
The Information Security Policy is a set of Procedures that apply to all information which the Colleges Group processes, irrespective of ownership or form.

Structure
The Information Security Policy document is in accordance with the recommendations set out in the "UCISA Information Security Toolkit" which in turn, is based on the control guidelines set out in the industry standard ISO 27001.

Information Security Principles

- Information will be protected in line with all relevant Colleges Group policies and legislation, notably those relating to data protection, human rights and freedom of information.
- Information will be made available solely to those who have a legitimate need for access.
- All information will be classified according to an appropriate level of security.
- The integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.
- Compliance with the Information Security policy will be enforced.

Legislation relevant to Information Security Policy

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents

The Data Protection Act regulates the use of personal data by organisations. Personal data is defined as information relating to a living, identifiable individual.

The Act is underpinned by eight guiding principles:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act. (Data subjects have the right to gain access to their personal as held by the College)
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

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

The Freedom of Information Act gives individuals a right of access to information held by the Colleges Group, subject to a number of exemptions. Requests for information must be made in writing (email, letter or fax) but can be received by any member of staff at the College. Such requests must be responded to within 20 working days.

Privacy and Electronic Communications Regulations 2003
http://www.legislation.gov.uk/uksi/2003/2426/contents/made

Section 11 of the Data Protection Act allows individuals to control the direct marketing information they receive from organisations. The Privacy and Electronic Communications Regulations specifically regulate the use of electronic communications (email, SMS text, cold calls) as a form of marketing and allow individuals to prevent further contact.

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

RIPA regulates the powers of public bodies to carry out surveillance and investigation and also deals with the interception of communications.

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

The Copyright, Designs and Patents Act (CDPA) defines and regulates copyright law in the UK. CDPA categorises the different types of works that are protected by copyright, including:

1. Literary, dramatic and musical works;
2. Artistic works;
3. Sound recordings and films;
4. Broadcasts;
5. Cable programmes;
6. Published editions.

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

The Computer Misuse Act was introduced partly in reaction to a specific legal case (R v Gold and Schifreen) and was intended to deter criminals from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer. The Act contains three criminal offences for computer misuse:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or facilitate commission of further offences;
- Unauthorised modification of computer material.

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

The Human Rights Act puts the rights set out in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security – it provides a right to respect for an individual's "private and family life, his home and his correspondence", a right that is also embedded within the Data Protection Act.

Digital Economy Act 2010
http://www.legislation.gov.uk/ukpga/2010/24/contents

The Digital Economy Act regulates the use of digital media in the UK. It deals with issues such as online copyright infringement and the obligations that internet service providers (ISPs) have to tackle online copyright infringement.

Counter-Terrorism and Security Act 2015
http://www.legislation.gov.uk/ukpga/2015/6/contents

Accessing websites or other material which promotes terrorism or violent extremism or which seeks to radicalise individuals to these causes will likely constitute an offence under the Counter-Terrorism and Security Act 2015.

2. Compliance Procedure

This Compliance Procedure is part of the Information Security Policy and outlines the Colleges Group requirement to comply with certain legal and regulatory frameworks. The Information Security Policy is to be read in conjunction with the Groups ICT Security Policy and Data Protection Policy.

Compliance with legislation
The Group provides policy statements and guidance for staff and students in relation to compliance with relevant legislation to help prevent breaches of the Colleges Group legal obligations. However, individuals are ultimately responsible for ensuring that they do not breach legal requirements during the course of their work or studies.

Users of the Group's online or network services are individually responsible for their activity and must be aware of the relevant legal requirements when using such services.

The Colleges Group must comply with all relevant legal requirements whether such requirements are detailed in internal policies or not. Any suspected breach of the Colleges Group legal requirements must be reported to the Director of IT Services.

Other regulatory requirements are set out below.

JANET policies
The Group, along with other UK educational and research institutions, uses the 'JANET' (Joint Academic NETwork) electronic communications network and must therefore comply with JANET's Acceptable Use and Security Policies. Both of these policies are available from the JISC website.

Payment Card Industry Data Security Standard (PCI DSS)
The Group must comply with the Payment Card Industry Data Security Standard (PCI DSS) when processing payment (credit/debit) cards.

Software Licence Management
All software used for Colleges Group business must be appropriately licensed. The Group must comply with the software and data licensing agreements it has entered into. During the negotiation process of such agreements, full consideration must be given to how compliance with the agreement can practically be achieved. Agreements may need to be specifically negotiated to enable the Colleges Group to comply.

Third party Terms and Conditions
Where the College uses the services of a third party provider, staff and students will also be subject to their terms and conditions in so far as they relate to information security.

Compliance with the Group Information Security Policy
The Colleges Group's Information Security Policy must be adhered to at all times when handling information and the Colleges Group must ensure it is acting legally when operating such policies.

All staff, students and other persons who may handle Colleges Group information must be made aware of the Group's Information Security Policy and of any amendments made to it. Individuals by using

Group Systems must understand that it is assumed that they have read and understood the Colleges Group policies and how they apply to the information they handle.

Collection of Evidence
At times, it may be necessary for the Colleges Group to collect evidence in relation to a potential legal claim or internal investigation.

Where there is suspicion of a criminal offence involving the Group's information or systems, the Group will cooperate with the relevant agency to assist in the preservation and gathering of evidence on the basis of appropriate internal authorisation and compliance with relevant statutory requirements.

Records Management
The Group is required to retain certain information, whether held in hard copy or electronically, for legally defined periods. Such information must be appropriately safeguarded and not destroyed prior to the defined minimum retention period, while remaining accessible to those who require access and are authorised to access that information.

In accordance with the Data Protection Act, personal data should not be retained for longer than it is required for the purposes for which it was collected.

3. Outsourcing and Third Party Procedure

This Procedure is part of the Information Security Policy and outlines the conditions that are required to maintain the security of the Group's information and systems when third parties, other than the Group's own staff or students, are involved in their operation.

Scope
This policy applies to any member of the Colleges Group who is considering engaging a third party to supply a service where that service may involve third party access to the Group's information assets. It also applies to any third parties who may have access to the Group's non-public information or systems for a specified purpose. This third party access could occur in a number of scenarios, common examples being:

- The use of cloud computing services;
- When third parties are involved in the design, development or operation of information systems for a College;
- When third party access to the Group's information systems is granted from remote locations where computer and network facilities may not be under the control of the Group;
- When users who are not members of the Group are given access to information or information systems.

Managing Outsourcing Risk
Prior to outsourcing or allowing a third party access to the Group's non-public information or systems, a decision must be taken by staff of appropriate seniority that the risks involved are clearly identified and acceptable to the College. The level of staff seniority will depend on the nature and scale of the outsourcing. Advice should be sought from the Director of IT Services during the decision making process.

Formal Outsourcing
Where a service is formally outsourced by the Colleges Group, the process must be managed by the relevant Group staff and a contract must be in place that covers standards and expectations relating to information security (see 'Contractual issues').

Due Diligence
The process of selecting a third party service provider must include due diligence of the third party in question, a risk assessment and a review of any proposed terms and conditions to ensure that the Colleges Group is not exposed to undue risk. This process may involve advice from members of the Group with expertise in contract law, IT, information security, data protection and human resources.

This process must also include the consideration of any information security policies or similar information available from the third party and whether they are acceptable to the Colleges Group.

Contractual Issues
All third parties who are given access to the College's non-public information or systems must agree to follow the information security policies of the Group. Advice should be sought from the Director of IT Services in relation to contractual arrangements.

Confidentiality clauses must be used in all contractual arrangements where a third party is given access to the Group's non-public information.

Use of third party services must not commence until the Colleges Group is satisfied with the information security measures in place and a contract has been signed.

All contracts with external suppliers for the supply of services to the Group must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

Data Protection Act
A Privacy Impact Assessment (PIA) must be completed at the outset of any project that will potentially involve personal data being accessed by a third party. Any outsourcing arrangement involving the transfer of personal data to a third party must include the acceptance of the Colleges Group standard personal data processing terms.

If the outsourcing involves the transfer of personal data outside the European Economic Area (EEA), it must only be to a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The Information Commissioner's Office (ICO) provides a list of countries it has deemed to provide an adequate level of protection. If the transfer is to the USA, the company or organisation must be signed up to the US-EU Safe Harbour scheme (or equivalent) for the duration of the contract.

Informal Outsourcing
There are extensive IT services that are available to members of the College via the internet which the College will have no formal agreement or contract in place with - examples include email services and cloud storage providers. Users of such services are required to accept the provider's set terms and conditions and the Colleges Group has no ability to negotiate as it would via the formal outsourcing procedure.

The use of such services for storing information present a real risk to the Group as there is no way the Group can ensure the confidentiality, integrity and availability of the information without a formal agreement in place. The storage of personal data with such providers is likely to be a breach of the Data Protection Act for which the Colleges Group could be penalised by the Information Commissioner.

In light of these risks, wherever possible, Group staff should only use services provided or endorsed by the Colleges Group for conducting Group business. The Group recognises, however, that there are occasions when it is unable to meet the legitimate requirements of its members and that in these circumstances it may be permissible to use services provided by other third parties.

Colleges Group data which is subject to the Data Protection Act or which has a classification of confidential or above should be stored using Group facilities or with third parties subject to a formal,

written, legal contract with the Colleges Group. In cases where it is necessary to otherwise remove data from the Group, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Further advice is available from IT Services.

Group staff must not configure their Colleges Group email account to automatically forward incoming mail to third party services with which the College has no formal agreement.

Third Party Physical Access

A risk assessment must be completed prior to allowing a third party to have access to secure areas of the College where confidential information and assets may be stored or processed. This assessment should take into account:

- what computing equipment the third party may have access to;
- what information they could potentially access;
- who the third party is;
- whether they require supervision;
- whether any further steps can be taken to mitigate risk.

4. Information Handling Procedure

Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur.

Inventory and Ownership of Information Assets
An inventory of the Colleges Group main information assets will be maintained and the ownership of each asset clearly stated.

Security Classification
Each information asset will be assigned a security classification which reflects the sensitivity of the asset according to the following classification scheme:

1. Public – available to any member of the public without restriction.
2. Open – available to any authenticated member of the College.
3. Confidential – available only to specified members, with appropriate authorisation.
4. Strictly Confidential – available to only a very small number of members, with appropriate authorisation.

Any information which is disclosable under the Freedom of Information Act 2000 will be classified as public. Any data which is classified as sensitive personal data under the Data Protection Act 2018 will be classified as strictly confidential. Any information which is not explicitly classified will be classified as open, by default.

Access to Information
Members of the Colleges Group will be granted access to the information they need in order to fulfil their roles within the Group. Members who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

Disposal of Information
Great care needs to be taken to ensure that information assets are disposed of securely.

Confidential paper waste must be disposed of in accordance with formal Colleges Group procedures.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the Colleges Group, unless the disposal is undertaken under contract by an approved contractor.

In cases where a storage system (for example a computer disc) is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the Group until it is disposed of securely.

Removal of Information
Group data which is subject to the Data Protection Act or which has a classification of confidential or above should be stored using Group facilities or with third parties subject to a formal, written legal contract with the Colleges Group, wherever possible. In cases where it is necessary to otherwise remove data from the Group, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss.

Using Personally Owned Devices
Any processing or storage of College Group information using personally owned devices must be in compliance with the Colleges Group ICT Security Policy.

Information on Desks, Screens and Printers
Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

Backups
IT Services will ensure that appropriate backup and system recovery measures are in place for Information that is entrusted to the care of IT Services. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures will be tested on a regular basis.

Exchanges of Information
Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Regular exchanges must be covered by a formal written agreement with the third party.

Hard copies of information classified as strictly confidential must only be exchanged with third parties via secure (for example, special) delivery.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Members of the Colleges Group must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

5. Network Management Procedure

Scope
All of the Colleges Group communications networks, whether wired or wireless are in scope, irrespective of the nature of the traffic carried over the networks (data or voice).

Management of the Network
The Colleges Group communications networks will be managed by suitably skilled staff to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability).

IT Services staff are in highly privileged positions and play a key role in contributing to the security of the Group's information assets. They are expected to be aware of the Colleges Group Information Security policy in its entirety and must always abide by the policy.
Infrastructure staff are authorised to act promptly to protect the security of the networks, but must be proportionate in the actions which they take, particularly when undertaking actions which have a direct impact on the users of the network. IT Services staff must immediately report any information security incidents to the Director of IT Services and/or Head of Infrastructure.

Network Design and Configuration
The network must be designed and configured to deliver high levels of performance, availability and reliability, appropriate to the Group's business needs, whilst providing a high degree of control over access to the network.

The network must be segregated into separate logical domains with routing and access controls operating between the domains in order to prevent unauthorised access to network resources and unnecessary traffic flows between the domains.

Physical Security and Integrity
Networking and communications facilities, including wiring closets, data centres and computer rooms must be adequately protected against accidental damage (fire or flood, for example), theft, or other malicious acts.

The network should, where appropriate and possible, be resilient to help mitigate the impact of the failure of network components.

Change Management
All changes to network components (routers, firewalls etc) are subject to IT Services established change management processes and procedures.

Connecting Devices to the Network
It is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the Colleges Group wireless networks.

Any device connected to a College network must be managed effectively. Devices which are not will be liable to physical or logical disconnection from the network without notice.

All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing, in accordance with normal IT Services operational practices.

Network Address Management
The allocation of network addresses (IPv4 and IPv6) used on the Group's networks shall be managed by IT Services' Infrastructure Team, which may delegate the management of subsets of these address spaces to other teams within IT Services.

Network addresses (IPv4 or IPv6) assigned to end-user systems will, wherever possible, be assigned dynamically (and will therefore be subject to change).

Access Controls
Access to network resources must be strictly controlled to prevent unauthorised access. Access control procedures must provide adequate safeguards through robust identification and authentication techniques.

IT Services is responsible for the management of the gateways which link the Colleges Group networks to the Internet. Controls will be enforced at these gateways to limit the exposure of Group systems to the Internet in order to reduce the risks of hacking, denial of service attacks, malware infection and propagation as well as unauthorised access to information. Controls will be applied to both incoming and outgoing traffic.

6. Software Management Procedure

Definitions
Software management - any procurement, development, installation, regulation, maintenance or removal of software that takes place on computers owned by, managed by or for the Colleges Group.

Computers - includes all end user computing devices, including tablets and smartphones, as well as Servers, whether or not they are on a College site.

General Software Management Principles
All software, including operating systems and applications must be actively managed.

There must be an identifiable individual and deputy, or organisational unit, taking current responsibility for every item of software formally deployed. Individuals installing software themselves are responsible for that installation. Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.

IT Services are responsible for ensuring the on-going security of the Colleges Group supplied software and will apply security patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches will either be applied within 3 working days of release or other compensatory control measures taken to mitigate risk. Standard Patches will be applied within 90 days of release.

Software Procurement
When business requirements for new systems or enhancements are being specified, the specification documents should describe any special or essential requirements for security controls. These could include manual controls required during operation.

When software for use by the Colleges Group is being procured there must be an assessment of whether the software incorporates adequate security controls for its intended purpose.

It must be investigated and taken into account whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.

At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.

Software Installation
Checks should always be made that there is a valid licence before installing software and users advised of any special conditions regarding its usage.

Automated installs should be used wherever possible - in line with current procedures.

Media / files must be stored securely and managed.

Software must not be put into user service on Colleges Group systems unless IT Services has assessed

and committed to providing sufficient resourcing for its ongoing management and support. Appropriate assessment / tests should be made to avoid new software causing operational problems to other systems on the network.

Individual users installing software on their own computers do so at their own risk.

Change control procedures must be followed and proper records maintained.

Software Regulation
Use or installation of unlicensed software and using software for illegal activities could be construed to be a disciplinary offence.

Use of software which tests or attempts to compromise Group systems or network security is prohibited unless authorised by the Director of IT Services.

Use of software which causes operational problems that inconvenience others, or which makes demands on resources which are excessive or cannot be justified, may be regulated or prohibited.

Software found on any Colleges Group system which incorporates malware of any type is liable to automated or manual removal or deactivation.

Software Removal
Software that is not licence compliant must be brought into compliance promptly within 5 working days or uninstalled.

Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service as soon as identified. Change control processes and procedures must be used, commensurate with the risk

When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence.

Permitted, Regulated and Prohibited Use of Software
The College must comply with its overriding legal and contractual obligations. Some of these obligations affect software and the uses to which it may be put. The Director of IT Services has responsibility for IT across the Colleges Group and this may include the prohibition of particular software.

7. Investigation of Computer Use Procedure

Scope
All members (staff, students and associates) of the Colleges Group together with any others who may have been granted permission to use the Group's information and communication technology facilities by the Director of IT Services are subject to this policy.

The College's Powers to Access Communications
Authorised staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or provided by the Group and may examine the content of these files and any relevant traffic data.

The Colleges Group may access files and communications for the following reasons:

1. To ensure the operational effectiveness of its services (for example, the Group may take measures to protect its systems from viruses and other threats).
2. To establish the existence of facts relevant to the business of the institution (for example, where a case of suspected plagiarism is being investigated and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent with the authority of an authorised person).
3. To investigate or detect unauthorised use of its systems.
4. To ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the Colleges Group business.
5. To monitor whether or not communications are relevant to the business of the Group (for example, checking email accounts when staff are absent on holiday or on sick leave to access relevant communications).
6. To comply with information requests made under the Data Protection Act or Freedom of Information Act (individuals would in normal circumstances be notified).

The Powers of Law Enforcement Authorities to Access Communications
A number of other non-College bodies and persons may be allowed access to user communications under certain circumstances. Where the Colleges Group is compelled to provide access to communications by virtue of a Court Order or other competent authority, the Group will disclose information to these non- institutional bodies/persons when required as allowed under the Data Protection Act 2018.

For example, under the Regulation of Investigatory Powers Act 2000 a warrant may be obtained by a number of law enforcement bodies regarding issues of national security, the prevention and detection of serious crime or the safeguarding of the economic well-being of the UK.

Other Third Parties
The Colleges Group makes use of third parties in delivering some of its IT services. These third parties may intercept communications for the purpose of ensuring the security and effective operation of their service (for example, a third party which provides email services to the Group may scan incoming and outgoing email for viruses and spam).

Covert Monitoring

Covert monitoring of computer use will only be authorised in exceptional circumstances where there is reason to suspect criminal activity or a serious breach of Colleges Group regulations and notification of the monitoring would be likely to prejudice the prevention or detection of that activity. The period and scope of the monitoring will be as narrow as possible to be able to investigate the alleged offence and the monitoring will cease as soon as the investigation is complete. Only information gathered in relation to the alleged offence will be retained. This information will only be viewed by those for whom access is strictly necessary, for example in relation to potential disciplinary proceedings.

8. User Management Procedure

Scope
All information systems used to conduct Colleges Group business, or which are connected to the Group's network must be managed in accordance with this procedure.

Eligibility
User accounts will only be provided for:

- Current Group staff and students.
- Students retaking Exams.
- Students waiting to graduate.
- Guests of the Colleges Group who may be granted temporary access to the Group's network.
- Visitors to the Colleges Group who may be granted temporary access to the Group's wireless networks.

Authorisation to manage
The management of user accounts and privileges on the Group's information systems is restricted to suitably trained and authorised members of staff.

Account and privilege management
Accounts will only be issued to those who are eligible for an account and whose identity has been verified.

When an account is created, a unique identifier (userID) will be assigned to the individual user for his or her individual use. This userID may not be assigned to any other person at any time.

On issue of account credentials, users must be informed of the requirement to comply with the Colleges Group Information Security Policy and ICT Security Policy.

Access rights granted to users will be restricted to the minimum required in order for them to fulfil their roles.

Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (e.g. when a member of staff changes their role or a member of staff or student leaves the Colleges Group).

Privileged accounts are accounts used for the administration of information systems and are distinct from user accounts. These accounts must only be used by system administrators when undertaking specific tasks which require special privileges. System administrators must use their user account at all other times.

9. System Management Procedure

Scope
The Group's computer systems will be managed by suitably skilled staff to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability). This procedure applies to all members of staff who use administrator (or elevated) privileges on any Colleges Group multi-user computer system (server) to administer the system or the services running on the system. The management of desktop systems is not in scope.

Duties and Responsibilities
System and Service managers are in uniquely privileged positions and play a key role in ensuring the security of the Group's systems and services. They are expected to be aware of the Group's Information Security Policy in its entirety and must always abide by the policy.

System managers should assign a business criticality level to their systems and ensure that their systems are registered with IT Services'. System managers are responsible for ensuring appropriate business continuity measures are in place to protect against events which might otherwise result in loss of service.

System managers should deploy systems to agreed secure baselines (systems will be "hardened"). Baselines will be agreed with IT Security specialists and will be defined for hypervisors (where relevant), operating systems, applications and any required "middleware". Baselines must be reviewed from time to time.

System managers are also responsible for ensuring the on-going security of their systems and must apply software patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches must be applied in accordance with software suppliers' recommendations (or requirements) or within 3 working days of release, whichever is the shorter. If it is not possible to patch within this time period, other compensatory control measures must be taken to mitigate risk.

Managers are authorised to act promptly to protect the security of their systems, but must be proportionate in the actions that they take, particularly when undertaking actions which have a direct impact on the users of their systems. System managers must immediately report any information security incidents to the Director of IT Services and/or Head of Infrastructure.

Change Management
All changes to computer systems are subject to IT Services' established change management processes and procedures.

Access Control
Access to all computer systems must be via a secure authentication process, with the exception of read-only access to publicly available information.

Access must only be granted in strict accordance with the User Management procedure. Administrator accounts and accounts with elevated privileges must only be used when necessary in order to undertake specific tasks which require the use of these accounts. At all other times, the principle of

"least privilege" should be followed.

Monitoring and Logging
The use and attempted use of all computer systems will be logged by IT Services. The data logged will be sufficient to support the security, compliance and capacity planning requirements of the system but should not be unnecessarily intrusive. The Data Protection Act requires that any personal data collected is collected for specific purposes and that it should be deleted when it is no longer needed.

Vulnerability Scanning
All College systems are subject to regular vulnerability scans initiated by IT Services (at least every 12 months). These scans may be undertaken by appropriately skilled IT staff or by approved 3rd Party's (such as JISC).

System Clocks
All system clocks must be synchronised to reliable time sources.