Information Security Policy

Policy Name:	Information Security Policy
Policy Lead:	Senior Manager: Head of Information Systems
Category:	Staff
Statutory:	No
Published on Website (www.loreto.ac.uk):	No
Reviewed by:	SLT/Finance and General Purposes Committee
Approved by:	Finance and General Purposes Committee
Date Approved:	June 2025
Review Period:	3 years
Next Review Date:	June 2028

Table of Contents

Vision

Loreto College is centred in God, rooted in Christ and animated by the spirit of Mary Ward, the founder of the Institute of the Blessed Virgin Mary. Our vision is that it will be an educational community where each person has the experience of being loved and valued as a sacred individual created by a loving God; a community where students enjoy an enriching and liberating education that helps them grow into the fullness of life and empowers them to be men and women of courage who are alive to the needs of humanity and committed to making a better world.

Information Security Policy

Information is a vital asset to any organisation and this is especially so in a knowledge driven organisation such as Loreto Sixth Form College, where information will relate to learning, teaching, administration and management.

This policy is concerned with the management and security of Loreto College's 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 College processes, irrespective of ownership or form.

Information Security Principles

- Information will be protected in line with all relevant Colleges 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

https://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

https://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 college days.

Privacy and Electronic Communications Regulations 2003

https://www.legislation.gov.uk/uksi/2003/2426/contents/made

Individuals can 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.

Investigatory Powers Act 2016 (IPA 2016) and the Regulation of Investigatory Powers Act (RIPA) 2000. IPA and RIPA regulate 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

https://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

https://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

https://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

https://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

https://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.

Compliance

Compliance is part of the Information Security Policy and outlines the College's requirement to comply with certain legal and regulatory frameworks. The Information Security Policy is to be read in conjunction with the Data Protection Policy.

Compliance with legislation

The College provides policy statements and guidance for staff and students in relation to compliance with relevant legislation to help prevent breaches of the Colleges 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 College’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 College must comply with all relevant legal requirements whether such requirements are detailed in internal policies or not. Any suspected breach of the College’s legal requirements must be reported to the Head of Information Systems

Other regulatory requirements are set out below.

JANET policies

The College, 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 College 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 College business must be appropriately licensed. The College 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 College 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 College Information Security Policy

The College Information Security Policy must be adhered to at all times when handling information and the College must ensure it is acting legally when operating such policies.

All staff, students and other persons who may handle College information must be made aware of the Colleges Information Security Policy and of any amendments made to it. Individuals by using College Systems must understand that it is assumed that they have read and understood the College policies and how they apply to the information they handle.

Any data breach or IT security breach should be reported to the Head of Information Systems, Network Manager and the Data Protection Officer in accordance with the Data Protection Policy.

Collection of Evidence

At times, it may be necessary for the College to collect evidence in relation to a potential legal claim or internal investigation.

Where there is suspicion of a criminal offence involving the College’s information or systems, the College 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 College 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

Outsourcing

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

Scope

This policy applies to any member of the College who is considering engaging a third party to supply a service where that service may involve third party access to the Colleges information assets. It also applies to any third parties who may have access to the College'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 College's information systems is granted from remote locations where computer and network facilities may not be under the control of the College;
- When users who are not members of the College are given access to information or information systems.

Managing Outsourcing Risk

Prior to outsourcing or allowing a third-party access to the College'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 Head of Information Systems during the decision-making process.

Formal Outsourcing

Where a service is formally outsourced by the College, the process must be managed by the relevant College 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 College is not exposed to undue risk. This process may involve advice from members of the College 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 College.

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 College. Advice should be sought from the Head of Information Systems in relation to contractual arrangements.

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

Use of third-party services must not commence until the College 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 College 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 Data Protection Impact Assessment (DPIA) 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 College standard personal data processing terms. This should be in line with the College Data Protection Policy.

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. Where data is being transferred outside of the EEA we will carry out due diligence to ensure that the country has similar safeguards and securities to those under the UK GDPR. Where this is not the case an impact assessment will be undertaken and data subjects informed.

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 College 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 College as there is no way the College 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 could be penalised by the Information Commissioner.

In light of these risks, wherever possible, College staff should only use services provided or endorsed by the College for conducting College business. The College 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.

College data which is subject to the Data Protection Act, or which has a classification of confidential or above should be stored using College facilities or with third parties subject to a formal, written, legal contract with the College. In cases where it is necessary to otherwise remove data from the College, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Further advice is available from IT Services.

College staff must not configure their College 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

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

All access to college systems is password protected and all staff access to Office 365 is protected by multi-factor authentication. All college owned laptops are encrypted. Any external storage, such as external hard drives or USB memory sticks, connected to the college network must be encrypted before any information can transferred to them.

Access to Information

Staff of the College will be granted access to the information they need in order to fulfil their roles within the College. Staff 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 College procedures. Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the College, 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 College until it is disposed of securely.

Removal of Information

College data which is subject to the Data Protection Act should be stored using College facilities or with third parties subject to a formal, written legal contract with the College, wherever possible. In cases where it is necessary to otherwise remove data from the College, 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 information using personally owned devices must be in compliance with the college's BYOD Agreement~~s~~.

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

Cross College IT (CCIT) 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 agreement with the third party.

Hard copies of information classified as strictly confidential must only be exchanged with third parties 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 College must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

Network Management

Scope

All the College communications networks, whether wired or wireless are in scope, irrespective of the nature of the traffic carried over the networks (data or voice). This includes usage of any cloud systems used.

Management of the Network

The College 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).

CCIT staff are in highly privileged positions and play a key role in contributing to the security of the College's information assets. They are expected to be aware of the College Information Security policy in its entirety and must always abide by the policy.

CCIT 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. CCIT staff must immediately report any information security incidents to the Head of Information Systems or the Network Manager.

Network Design and Configuration

The network must be designed and configured to deliver high levels of performance, availability and reliability, appropriate to the College'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 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 CCIT established change management processes and procedures.

Connecting Devices to the Network

All personal devices connecting to the network must adhere to the college's BYOD agreement. It is permissible to connect personally owned equipment to the Colleges wireless networks. Any wired connections must be approved by the Network Manager.

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 CCIT operational practices.

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.

CCIT is responsible for the management of the gateways which link the College networks to the Internet. Controls will be enforced at these gateways to limit the exposure of College 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

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 College.

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, or organisational unit, taking current responsibility for every item of software formally deployed. 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.

CCIT or the responsible individual or organisational unit are responsible for ensuring the on-going security of the College 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). Critical security patches will be applied as soon as possible but within 28 days of release. ~~High priority patches will either be applied as soon as possible 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 College 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 considered 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.

Media / files must be stored securely and managed.

Software must not be put into user service on College systems unless CCIT 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.

Software Regulation

Use of software must comply with the Staff/Governor/Students ICT User Agreements.

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 College systems or network security is prohibited unless authorised by the Head of Information Systems.

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 College 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 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.

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 Head of Information Systems has responsibility for IT across the college, and this may include the prohibition of particular software.

7. Investigation of Computer Use

Scope

All members (staff, students and associates) of the College together with any others who may have been granted permission to use the College's information and communication technology facilities by the Head of Information Systems 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 College and may examine the content of these files and any relevant traffic data.

The College may access files and communications for the following reasons:

1. To ensure the operational effectiveness of its services (for example, the College 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, or AI misuse, 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 College business.
5. To monitor whether or not communications are relevant to the business of the College (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 College is compelled to provide access to communications by virtue of a Court Order or other competent authority, the College will disclose information to these non- institutional bodies/persons when required as allowed under the Data Protection Act 2018.

For example, under IPA / RIPA 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 College 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 College may scan incoming and outgoing email for malware and spam).

8. User Management

Scope

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

Eligibility

User accounts will only be provided for:

- Current College staff, students and governors
- Guests of the College who may be granted temporary access to the College network
- Visitors to the College who may be granted temporary access to the College's wireless networks

Authorisation to manage

The management of user accounts and privileges on the College'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 College's Information 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 College).

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

Scope

The College'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 applies to all members of staff who use administrator (or elevated) privileges on any College multi-user computer system (server) to administer the system or the services running on the system

Duties and Responsibilities

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

The Network Manager is responsible for ensuring appropriate business continuity measures are in place to protect against events which might otherwise result in loss of service.

The Network Manager is 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) If it is not possible to patch within this time period, other compensatory control measures must be taken to mitigate risk.

The Network Manager is 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. The Network Manager must immediately report any information security incidents to the designated Data Protection Officer.

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.

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 CCIT. 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 the Network Manager (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.

ID Cards

All staff and students carry ID cards which are checked by the security staff on entering the college. The ID cards are encoded to restrict access to certain areas as appropriate.

Related Policies / Agreements

- Data Protection Policy
- Safeguarding Policy
- Online Safety Policy
- Staff and Governors ICT User Agreement
- Student ICT User Agreement
- Bring Your Own Device (BYOD) Agreement
- Social Media Policy
- CCTV Policy