ICT NETWORK SECURITY POLICY

Process Area	**Business Systems**
Reference Number	**BUS/005**
Directorate	**Finance and Planning**

Issue No	Date	Details	Author	Approved
001	Jun 2009	First issue	ST/JO'H	BD
002	Jan 2014	Changes to Sections 4.2.1 & 4.3	ST/KK	BD
003	Jan 2017	Reviewed by KK/ST – no changes recommended.	ST/KK	Governing Body
004	Dec 2019	Reviewed by ST/TS – Changes for Identity/Access Control strengthened plus separate Procedural Note.	ST/TS	Governing Body
005	Oct 2022	References to technical controls added in relation to remote access. Approvals for staff remote access updated.	LC, ST/TS	Governing Body

If requested, the College will make the policy available in alternative formats to accommodate visual impairments. The policy can also be downloaded from the College website and made available in alternative languages upon request.

1 POLICY STATEMENT

The aim of this policy is to state the principles which govern the security of the College's Information and Communications Technology (ICT) network, which includes the educational and MIS systems and platforms. The College is heavily dependent on information and information systems for all of its activities. The importance of the data, the systems used for processing and communicating data and the technological base on which these sits, make it essential that effective security measures are in place and observed.

There is an obligation on the part of all users who have access to the College's network to take an active part in security and this policy will help all authorised users to understand and fulfil their responsibilities where the use and security of the College's network is concerned. Individuals who do not play their part in security procedures place others and the College at risk.

This Policy has been developed to protect the availability and integrity of ICT systems in support of the College's activities and to provide a framework for ICT and network security across the organisation.

Access to all information will be controlled and will be driven by business requirements. Access will be granted or arrangements made for users according to their role, only to a level that will allow them to carry out their duties.

This policy will be reviewed and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies, contractual obligations or technological advances.

2 SCOPE

The policy applies to all staff, students and other persons (e.g. Governors, contractors and visitors) with access to College data and/or information systems. The policy applies to all types of data (paper-based and electronic) and information and communications technology systems comprising the College's network.

This policy addresses both the infrastructure and those common core systems that rely on the network to operate. The role of the network is to provide staff and students with a data communications platform, which supports all of the SRC business requirements.

Failure to comply with this Policy will be treated as a disciplinary offence.

3 DEFINITIONS

Incident	A security incident is an event that may indicate that an organisation's systems or data have been compromised or that measures put in place to protect them have failed.
IT Security Breach	A security breach is any incident that results in unauthorised access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.

4 ROLES AND RESPONSIBILITIES

ICT Network Security Responsibilities

Chief Executive

The Chief Executive is responsible for:

- ensuring guidance and procedural notes are approved in accordance with College governance arrangements for issue to staff;
- approving all requests for remote access to College systems from both staff and third parties;

Director of Finance and Planning

The Director of Finance and Planning is responsible for:

- providing clear direction and visible senior management support for all security initiatives;
- acting as the Senior Information Risk Officer (SIRO) and has overall responsibility for managing a culture for protecting information and ensure compliance with referred legislation.
- promoting security through appropriate commitment and adequate resourcing, in conjunction with the SMT and relevant personnel;
- deputising, as required, for the Chief Executive in respect of ICT security responsibilities; and
- ensuring compliance with relevant Data Protection legislation and GDPR regulations.

Assistant Director for ILT Development and ILT Systems

The Assistant Director for ILT Development and ILT Systems is responsible for:

- ensuring ICT network security risks are being managed effectively;
- ensuring all staff and students are aware of their responsibilities for network security and any related guidance notes;
- ensuring staff and students have an awareness of the Computer Misuse Act 1990 and other relevant legislation;
- ensuring the Network Security Policy is reviewed regularly;

Head of ICT and Network Services

The Head of ICT and Network Services will be responsible for:

- maintaining a register of the College's Information Systems including details of system owners;
- determining the appropriate level of security and the measures that must be applied to information systems;
- operating a risk management process to ensure ICT network security risks are managed effectively;
- ensuring contractors and their employees have a proper awareness and concern for the security of college information;

- applying standards, procedures and facilities for implementing computer systems security, including virus controls and passwords;
- reviewing the ICT Network Security Policy regularly or when there are significant changes or updates required to it;
- investigating and documenting all breaches of Network Security, actual or suspected and keeping the Chief Executive and Director of Finance and Planning advised as appropriate;
- ensuring Core Hardware is housed in a controlled and secure environment;
- ensuring that access to secure network areas is properly controlled and monitored;
- ensuring that logon access to the network is properly controlled and monitored;
- ensuring that 3rd Party requests for access to the network are approved by the Chief Executive and that such access is properly controlled with appropriate audit trails and is monitored on a regular basis;
- ensure that staff requests for remote access are approved in line with the technical controls and managed with appropriate audit trails and monitored on a regular basis;
- ensuring that network faults are logged and action taken to resolve them;
- ensuring that documented procedures are prepared for the operation and security of the ICT network;
- ensuring that appropriate backup and restoration procedures for all network systems are in place and are regularly tested;
- ensuring that an appropriate Business Continuity and Disaster recovery plan is in place; and
- ensuring all staff and students have an awareness of the Data Protection Act.

Head of MIS

The Head of MIS is responsible for:

- ensuring logon access to the College MIS systems is properly controlled;
- ensuring data exchange with external organisations is approved and carried out securely;
- operating effective change control processes in respect of the college information systems incorporating approval, testing and formal acceptance; and
- advising the Head of ICT and Network Services of any incidents that compromise, or have the potential to compromise the security of the SRC network.

Head of Human Resources

The Head of Human Resources is responsible for:

- ensuring all staff are aware of their personal accountability and responsibility with regard to ICT network security and failure to comply with the ICT Network Security Policy will be treated as a disciplinary offence;
- ensuring a formal, documented user registration and de-registration procedure for access to the network is followed; and
- ensuring a formal procedure for communicating changes in job roles is followed.

Section Managers (Information Owners)

Section Managers with specific 'Line of Business' applications within their department must ensure:

- information security remains a priority;
- access to College information is appropriately authorised and a suitable authorisation process is followed;
- risks to information security are identified and regularly reviewed;
- regular access reviews are carried out;
- ensure user roles and responsibilities are clearly defined and ensure that access to the College's Information Systems is limited to those users who have the necessary authority and clearance;
- they are aware of their responsibilities as an information owner and ensure appropriate controls are in place to protect the information they are responsible for;
- the College policy with regard to passwords is implemented and complied with; and
- that specific controls are implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

Line Managers

All managers are responsible for:

- implementing the policy within their business areas, and for ensuring compliance by their staff;
- deputising for Information Owners to approve individual user requests for access to network resources;
- notifying ICT and Network Services of any changes in an employee's job role so that permissions can be updated;
- ensuring that staff and as appropriate students, are made aware of their security responsibilities;
- reporting, promptly, to the Head of ICT and Network Services any breaches of network security;
- enforcing disciplinary procedures with students who are deemed to be in breach of Network Security;
- ensuring they review and approve any requests for Remote access to the network and ensure they are approved by Head of IT and that such access is properly controlled with appropriate audit trails and is monitored on a regular basis;
- ensuring requests to borrow equipment are authorised; and
- ensuring any equipment issued to staff is returned.

All managers with responsibility for a particular information system, or information technology area (e.g. ILT, Open Source) are responsible for taking appropriate steps to ensure the integrity and security of those systems in line with this policy.

All staff

Whilst staff may be permitted remote access to college network systems, it is the responsibility of each employee to adhere to this policy ensuring that **all** the information (s)he manages shall be appropriately secured to protect against identified risks, whether in or out of college.

Remote access will only be granted upon completion of a staff request for remote access available on the IT SharePoint Site. Technical controls will be implemented to ensure that user accounts and user devices meet the required standard before access is permitted. To promote the security of all College information, staff should only download or copy information if it is necessary to allow them to complete their job role. Appropriate steps must be taken to protect the integrity of such information and to prevent access or use of it by any unauthorised party.

All Users

Each system user is responsible for the security of hardware in their use and for the security of their use of the system. Faults and incidents must be reported to the Network Operations Manager via the appropriate incident reporting procedures (keeping line management advised and informed).

Any suspected IT security breach or misuse of a user account should be reported immediately to your line manager or Head of Faculty along with IT Services and the Data Protection Officer.

All users must ensure they protect the network from unauthorised access by logging off when finished working or locking the screen when they leave a machine unattended even for short periods of time.

Irresponsible or improper actions by users may result in disciplinary action.

External Contractors

All external contractors seeking access to college systems must agree to abide by the rules laid out in the request for 3rd party access document and be authorised by the Chief Executive, or nominated deputy.

5 PROCEDURES FOR IMPLEMENTATION

Nature of the College's Network

The College Network has been designed to support the operations of the College and for general use in a college environment, including storage and transmission of personal, financial and commercial data. Procedures are in place to protect the integrity of data stored and transmitted across the network; however it is important for users of the network to bear in mind the sensitivity of their data when storing and transmitting information and to take appropriate steps to ensure it is protected. Any concerns regarding the security of information should be directed to the Head of ICT and Network Services.

Security Threats and Countermeasures

Security countermeasures and mechanisms imposed on the network are designed to ensure:

- the confidentiality of data;
- the integrity and/or accuracy of data; and
- the availability of the service to users.

Specific Threats

The most likely causes of a compromise of Confidentiality are:

- communications interception by third parties;
- use of inappropriate storage mediums for confidential data, i.e. Public Cloud technologies/services e.g. Dropbox
- careless handling of data storage devices, e.g. pen drives, laptops, failure to lock down PCs; and
- a masquerading attack by authorised users (including a third-party contractor) and/or outsiders.

The most likely causes of a compromise of Integrity are:

- the introduction of damaging or disruptive software, e.g. a virus; and
- the embedding of malicious code.

The most likely causes of a compromise of Availability are:

- the introduction of damaging or disruptive software, e.g. a virus or untried or untested software;
- the technical failure of the network service;
- the technical failure of network distribution components;
- power failure;
- hardware maintenance error; and
- software maintenance error.

The threats listed above are those found to be the most likely to occur. They are not the only threats which need to be addressed. This policy and any guidance issued by IT Services is designed to address threats such as those described. All users of the College's network have a responsibility to ensure exposure to such threats is not increased or exacerbated through individual actions.

Security Countermeasures

The main security countermeasures flowing from this policy will include:

- Regular review of this Policy to take account of changes and developments to ensure it remains appropriate;

- Security Infrastructure - a management framework shall be established which will initiate and control the implementation of information security;

- Incident Handling - security incidents shall be detected, any damage managed, and lessons learnt and disseminated. This will include reporting of security weaknesses and software malfunctions;

- Outsourcing - third party access to organisational information processing facilities shall be based on formal arrangements;

- Compliance Checks - appropriate procedures shall be implemented to ensure compliance with legal, statutory, regulatory and contractual requirements;

- Passwords –All users must follow good security practices in the selection and use of passwords in accordance with the College's Password policy. Passwords should be changed regularly to assist in ensuring that the confidentiality and the integrity of the password continue to be maintained. It is the responsibility of individual users to maintain the integrity of their passwords;

- Physical Access Control -Site/Building physical security will be first line of defence against an external attacker trying to gain access. Appropriate physical security measures will be applied. Access to College Server Rooms is additionally restricted;

- Logical Access Control – Access to data is appropriately controlled using a range of methods. Access control methods used by default include:

    - explicit logon to devices;
    - Windows share and file permissions to files and folders;
    - user account privilege limitations;
    - server and workstation access rights;
    - firewall permissions;
    - network zone and VLAN ACLs;
    - IIS/Apache intranet/extranet authentication rights;
    - Database access rights;
    - Encryption at rest and in flight;
    - Conditional Access requirements.

- Applications – controls, procedures and protocols will be applied to maintain the integrity of application systems and data. Users will only be provided with direct access to the services that they have been specifically authorised to use;

- Diagnostic and control equipment must be physically protected and its use strictly controlled;

- Theft Protection measures will be put in place to prevent the theft of ICT assets and to detect occurrences of theft of ICT assets;

- Data/Information exchange – formal agreements should be established for the exchange of data including appropriate security measures, e.g. encryption of personal or sensitive data;

- Network management will be undertaken in a secure manner and should provide support for the management of network security. The status of the network shall be constantly monitored to allow for the early detection of unauthorised use, detection or failure and this will include mechanisms which minimise the effects of disruption to applications and services;

- Object/equipment reuse - there will be procedures to ensure that when data or sensitive software is deleted from ICT media it should be securely deleted, with no residue remaining, which could be recovered by unauthorised personnel;

- Reliability of Service – procedures and protocols will be established to ensure the reliability and integrity of systems and software before they are introduced to the live SRC network. This will include system and acceptance testing;

- Software and data Integrity - the integrity of software will be maintained in live use. This will include procedures to minimise the potential for the introduction of malicious software into the network. The network will be monitored for potential malicious software activity and any identified malicious software will be isolated and removed;

- Software Change Controls - All changes to software shall be authorised by the Head of ICT before being implemented. All changes to software must be recorded to support the change authorisation procedures. Any changes to software, which have to be made before the authorisation can be granted must be controlled and kept to a minimum;

- System Input / Output Controls - the identities of Input / Output devices will be determined to assist in enforcing this policy. In particular care must be taken when exporting information to another organisation to ensure the security and integrity of information and to ensure that the receiving organisation will provide the necessary level of protection to the information. Organisations and individuals receiving the information must be advised as to the sensitivity of the information so they can take appropriate measures;

- Network Resilience – the network is designed to be resilient and includes devices to manage and minimise failure or disruption. The status of the network will be monitored so that failures or errors can be detected quickly and rectified. This will include monitoring of the quality of network services;

- Software Maintenance Controls - the identity of software maintenance engineers and external contractors will be checked to reduce the risk of unauthorised people gaining access to systems and information;

- Business Continuity Plan will be developed to maintain or restore business operations in acceptable time scales following interruption to, or failure of, critical business processes; and

- Back-up of Data will be taken to ensure the continued availability of data.

6 DISTRIBUTION

SharePoint Policy Centre
College Web Site

7. RELATED DOCUMENTS

Some aspects of information security are governed by legislation and the most notable U.K. Acts are:

- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Data Protection Act 2018 (DPA 2018)
- United Kingdom General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000
- Copyright, Designs & Patents Act 1988
- Copyright and Trade Marks (Offences and Enforcement) Act 2002
- The Telecommunications Act (1984)
- The Electronic Communications Act (2000)

- Obscene Publication Act 1959 & 1964
- Protection of Children Act 1978
- The Defamation Act (1996 and 2013)
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Counter Terrorism and Security Act 2015
- Human Rights Act 1998
- Equality Act 2010
- Privacy and Electronic Communications Regulations 2003

** This list is not exhaustive and will be subject to change **

In addition, there are a number of other related policies, including:

- Freedom of Information Policy
- Network Acceptable Use Policy
- Data Protection GDPR Policy
- Information Handling Policy
- Mobile and Remote Working Policy
- Bring Your Own Device Policy
- Social Media Policy
- JANET Acceptable Use Policy

8. FLOWCHART

None