SERC

INSPIRING. TRANSFORMING. ENRICHING.

SOP NUMBER: 206-10-2015

ACADEMIC YEAR: 2020/2021 ONWARDS

DATE OF THIS ISSUE: June 2021

TITLE:

ICT Systems and Services SOP

Responsible Owner:

Chief Technology Officer

Summary of Contents

ICT Services Procedures:

- Access Control
- Anti-malware & Anti-Spyware
- Email and Messaging
- Internet Use
- Social Media
- Network Management
- Password
- Security
- Software Licensing Management
- Data Management
- Remote Access & Mobile Computing

List of ICT Systems Managers

First Created:
30 September 2015

Last CMT Approval Date:
2 June 2021

Review Information

Reviewed: October 2018
June 2019
May 2021

Next Review Due: May 2022

Requires CMT Approval (yes/no): Yes

Pervious Reference (for control purposes):

155-05-2014: ICT Systems and Services SOP

189-06-2015: Social Media SOP

Equality of Opportunity and Good Relations Screening Information (Section 75):

Date Procedure Screened – October 2016

Contents

1.0 Change History

Changes to this SOP are documented in Appendix 1 of this document. When reading electronic copies of this document, you can click here to view the change history.

2.0 Abbreviations

The definition of abbreviations used within this policy are as follows:

2FA (Two Factor Authentication), MFA (Multi Factor Authentication)
The process of verifying a user's identity at login using two or more security tokens. Typically, this is a username & password + another mechanism such as an SMS Text, Phone Call, Authentication app, Biometric Device (Fingerprint, Iris Scan, Facial Recognition) or smartcard. The 'Second' factor can be thought of as a second password.

CMT (College Management Team)
The senior management team within the college.

IdP (Identity Provider)
A system that is used to manage an organisations user accounts & password. These systems also provide identity protection, 3rd party integration & monitoring capabilities.

ICSC (Information & Cyber Security Committee)
The committee responsible for monitoring cyber & information security within the college.

ITS (IT & Services)
The college department responsible for the delivery of computing services at SERC.

JANET (Joint Academic NETwork)
JANET is the trademark used for the collection of networking services and facilities which support communication requirements of the UK education and research community. This service is provided by JISC.

JISC (formerly the Joint Information Systems Committee)
JISC is a UK higher, further education and skills sectors' not-for-profit organisation for digital services and solutions. It operates shared digital infrastructure and services, negotiates sector-wide deals with IT vendors and commercial publishers & provides advice and practical assistance for universities, colleges and learning providers.

SSD (Solid State Disk)
A storage device containing non-volatile flash memory, used in place of a hard disk because of its much greater speed.

SSO (Single Sign-On)
The process on logging into a system without having to re-enter a password. A typical example would be logging into a computer with a username & password, with access to other systems automatically granted by the initial login.

TLS (Transport Layer Security)
A cryptographic protocol designed to provide communications security over a computer network.

VPN (Virtual Private Network)
A VPN extends a private network across a public network such as the internet. It enables users to send and receive data securely across shared or public networks as if their computing devices were directly connected to the private network. VPN's are often used in remote working scenarios.

3.0 Background

The College regards Information systems and the information they contain, of vital importance to the efficient functioning of the organisation. The systems and the associated information processing tools and services – including desktop productivity tools, e-mail, web-based systems and the underlying network – now pervade all functions of the College.

Security of information is an essential requirement in any business or organisation. The procedures contained in this ICT Services SOP aim to ensure security of information.

The procedures should be followed in conjunction with the SERC Acceptable Use Policy.

4.0 Scope

These procedures apply to all authorised users of College information systems (staff, students and third-party users).

5.0 Access Control Procedure

5.1 Introduction

The business requirements for access controls on computer systems are:

- Protection of sensitive, personal or confidential information from unauthorised access.
- Ensuring data integrity in terms of preventing deliberate or accidental modification or deletion.

5.2 Access Control Rules

5.2.1 All Users

The College requires that authorised access to any computerised information system by staff, students or third parties must be controlled by an appropriate level of access.

The rules for access to computerised systems are as follows:

- Users can only be granted authorisation to shared information after approval has been given by an authorisation authority (i.e. tutor in case of students, Head of School or Unit in the case of staff).
- Access will be controlled via pre-determined access levels. Authorised users will be assigned the approved level of access by the system manager for the system that access is sought.
- Access granted must only be to very specific information and must not include any access to information that the user does not require access to.
- The type of access, (i.e. read, write etc.) in cases of access to shared information, must be established prior to granting access.
- Access is dependent upon each user having a unique computer user account and password. Creation of accounts for staff are dependent upon authorisation from Human Resources which includes completion of the College's Acceptable Use Policy.
- Student account creation is dependent upon enrolment on a College course and acceptance of the terms of the College's Acceptable Use Policy.
- User accounts of users who have changed job function, or who have left the College will be disabled upon notification from the Human Resources Department

5.2.2 Access Control Rules – System and Network Administrators

- System and network administrators will be permitted the highest access levels to information within their information system or domain provided that:
- Such access is required to administer and manage the information system, information store or network domain.
- Strict observance of data confidentiality is practised.
- Strong passwords are selected as per guidelines issued in the College Password Procedure (Section 11.0).

5.3 Types of Access Control Employed

The type of access control that will be used include:

5.3.1 Information System Controls

Each user must be given approval to have access to a system by the System Manager. The appropriate access level will be determined by the System Manager and agreed with the user's Head of School/Unit before the access level can be assigned.

5.3.2 File System Controls

Access to centralised file systems such as folders of documents on file or storage servers will be permitted via profiling and network security group access.

5.3.3 Computer System Controls

Use of security controls such as Microsoft's Group Policy will be used to control access to Personal Computer operating system files, admin tools and to prevent installation of software.

5.3.4 Network Controls

Protection of the College network will be achieved by the use of firewalls, access control lists and where appropriate VLANS (Virtual Local Area Networks). All IT devices that allow access to data, systems, and networks must contain a default 'deny all' inbound access rule. The only open ports should eb those that are required to complete the function of the device.

5.4 Monitoring and Review of Access

System and Network managers will review at least annually the access levels pre-configured for each system and also the access level that has been granted to each user for the information system, information store or network domain.

5.5 Reporting of Incidents

All users have a responsibility to report to appropriate system managers (see Appendix 2):

- Access still granted but no longer required to a system.
- Excessive or inappropriate access to a system.
- Misuse of access to a system by another user.

5.6 Requesting Access

Access will initially be assigned based upon departmental membership & organisational role. If further access is required to systems such as a SharePoint TeamSite or line of business application, this access may be requested by an authoritative line manager. Requests can be made as set out in section 40.

6.0 Security & Anti-malware Procedure

6.1 Introduction

The business critical dependence on ICT systems necessitates that appropriate support, security and contingency arrangements are in place to ensure system reliability and availability. One of the greatest risks to system stability and data integrity has been the growth in number and prevalence of malware software.

6.2 Definitions of Main Malware Types

- Virus - is a computer program designed to cause corruption or destruction of other computer applications and data. It usually infects an existing program
- Ransomware – is a program that encrypts data on the victim's computer. The perpetrator behind the attack issues instructions on how to recover the data. Usually payment is demanded in the form of a virtual currency such as bitcoins.
- Worm – is a computer program that replicates itself on the host computer and often will attempt to spread to computers on other networks.
- Trojan horse – is a computer program which disguises itself to appear useful or interesting in order to persuade a victim to install it. They can be used by criminal elements to create a "backdoor" to a computer for purposes of stealing personal or financial information, or to provide a means to have control of the infected computer.
- Spyware – is a computer program that records or captures information from an infected computer without the knowledge of the computer user

With the onset of web and e-mail services, malware can spread across multiple organisations and countries very quickly. The most common method of infection today is via infected file attachments on e-mail messages.

6.3 Susceptibility

Organisations most susceptible to infection, are those who either do not have any anti-malware or anti-spyware software, or who do not take adequate measures to ensure that the software is kept updated on servers and other IT devices. Furthermore, organisations who interchange information regularly between employees or indeed other organisations increase the likelihood of infection spreading.

6.4 Preventative Measures

The College uses a commercial anti-malware product that provides coverage for all servers, PCs and laptops. The product is updated on all servers and desktops directly when latest updates are available from the vendor's web site. The update status of all PC's is centrally monitored. Non-protected & out of date devices are proactively identified by the software.

It is not, however, acceptable to rely on the anti-malware product alone to prevent a viral outbreak. There are a number of mandatory stipulations to be observed by staff and students to ensure the risk of virus and spyware infections are kept to a minimum:

- All Servers, PCs and laptops and other ICT devices[1] brought on to any College Centre must be properly configured for automatic updates and have up to date anti-malware software installed.
- It is not permissible to attempt the interrupting or disabling of automatic updates to the anti-malware software.
- All College–owned laptops and PCs must be connected to the College network at least once per week to facilitate anti-malware updates.

- Personally owned laptops and PCs must be kept updated with anti-malware software particularly if such devices are used to interchange information with College systems.
- It is not permissible to copy/upload any material to any device on the College network unless that device (i.e. PC or laptop) has the most recent anti-malware updates installed. Advice should be sought from the IT & Services Department if staff or students have any doubts as regards the integrity of data stored on portable media regardless of the media having been previously scanned.
- Only software procured and installed by the College may be used on any College owned ICT device. Installation and execution of any other type of software, including screensavers and games is prohibited.
- Use of peer to peer file sharing programs is strictly forbidden i.e., Kazaa, Limewire, Bear Share, due to the extremely high risk of virus introduction.
- Installation or use of spyware software is forbidden.
- It is not permissible to download any software from any spyware websites.
- Unexpected or suspect e-mail messages with or without attachments must be deleted immediately. Care must also be taken to immediately empty the Deleted Items folder.
- All users should monitor 'IT announcements' email for new virus or spyware alerts and take appropriate action.
- Downloading of any file type from unsolicited web sites is prohibited.
- It is the responsibility of all users of College computing facilities to ensure that data stored on portable devices (i.e. laptops, Macbooks, tablets) or portable media such as USB drives or Smart Phones is backed up.
- The use of portable media is strongly discouraged. Users should consider using OneDrive for file storage, which brings protection in terms of backup, versioning and Malware/ransomware protections.
- Suspected virus infections must be reported immediately to the IT & Services Department.

[1] *Devices referrers to any type of tablet, mobile phones or any other device with processing and storage capability which can connect with any other ICT device.*

6.5 Levels of Protection

Having anti-malware protection on servers and desktops provides multi-level protection in that material sent via e-mail or the web is scanned on the e-mail/web server before being accessed by client PCs. Furthermore, material loaded via portable media[2] is scanned by the client PC and then scanned again by the anti-malware guarded file server.

All College servers including domain controllers, file servers, firewall and any other on-premise services must be protected with anti-malware software.

Additional protective measures include:

- Certain file types known to “hide” or contain viruses are blocked if included in e-mail attachments. Some examples include: .exe, .vbs, .com, .mdb.
- Macro security levels in the Microsoft Office suite are set to Medium or High.
- ICT devices run on a least privilege model with software installation restricted to ITS staff.

- Infected file attachments on external e-mail messages coming into the College are removed.
- Off-line content is deleted from PC/laptops after a successful login has taken place.

6.6 Monitoring & Reporting

There are 5 key tools that are used by ITS to monitor the health of the network. These are:

Microsoft Defender Security Centre
Defender Security centre monitors & manages the antimalware software on all workstations, servers & mobile devices. It also maintains an inventory of installed applications and any vulnerabilities. Finally, it will automatically notify administrative staff about any malware, unwanted software & suspicious program/user behaviour on devices.

Microsoft Cloud App Security
Cloud app security monitors user interaction with cloud-based services such as Office 365 and Azure AD. In addition, though the use on premise agents, it can also make security recommendations in relation to the on-premise network. Alerts raised here can be used by administrators to investigate suspicious account activity.

Azure Security Centre
Azure security centre is used to monitor user behaviour and can proactively block or disable accounts based in a risk assessment of risk.

Microsoft Endpoint Manager
Endpoint manager, formerly know as Intune, is a Mobile Device management solution used by the college to manage mobile phones, tablets and cloud based PCs. The solution contain a wealth of hardware & software inventory data as well as the ability to assess security compliance, assign policy and event remotely erase the device.

Microsoft 365 Security Centre
The Microsoft 365 security centre contains a recommendation engine that can be used to progressively improve the security profile of a network and any associated cloud services. It uses a rage of telemetry data from the 4 previous systems to provide a measure known as 'Secure Score'. Secure score is an important part of SERC's approach to ensuring the secure configuration of its network.

ITS staff proactively monitor the status of above solutions on a daily basis. When events such as malware detection, or unusual user activity occurs, ITS staff are notified immediately and are expected to investigate the cause.

Events relating to end user device should be investigated by staff in the ICT Technical Support Officer Role and logged in the desktop operations log.

Events relating to servers, network infrastructure and cloud services should be investigated by staff in the Network Manager Role and logged in the network operations log.

Whilst monitoring provides baseline security assurances, no level of monitoring will be 100% effective. Therefore, any indications or suspicions of virus/spyware activity must be reported to the College IT & Services Section at one of the local campuses: Bangor, Downpatrick or Lisburn.

6.7 Dealing with a Malware outbreak

Should a viral outbreak take place the following procedure will be followed:

- Chief Technology Officer to inform CMT, ICSC, Heads of School and Unit Heads of scope and scale of infection.
- ITS staff will attempt to isolate infected device(s). This may be achieved using Microsoft Defender Security Centre network isolation & app restriction features.
- If required, infected devices will be disconnected from the network.
- If required, unaffected network segments will be isolated from infected segments.
- Virus free devices with latest anti-malware software will be used as a cleaning medium for cleansing of infected files. If feasible, a secondary anti-malware product will be used to ensure that infected material and devices have been entirely cleansed.
- In parallel, all servers, PCs & laptops will be reviewed and if necessary, updated with the latest anti-malware updates.
- The “all clear” to be issued by the Chief Technology Officer to CMT, ICSC, Heads of School and Unit Heads.
- An incident should be recorded in the ICT Operations Log.
- In the event of a significant event, an Information Security Incident Report form should be completed, followed by an investigation by the Chief Technology Officer as to the cause of infection. On completion, a report is to be produced and forwarded to the ICSC, outlining a root cause analysis, details of any data loss or damage, appropriate countermeasures and future safeguards.

6.8 Deliberate Malware Introduction

Whilst malware by nature is created to deliberately disrupt ICT services, often they are accidentally introduced to an organisation’s ICT systems. These scenarios will be dealt with on a case by case basis. However, any employee or student who either deliberately introduces, or attempts to introduce malware, or who is complicit with other parties or individuals in introducing or attempting to introduce a virus or spyware software will be subject to disciplinary action. This activity will be treated as Gross Misconduct.

6.9 Liability

The College will not be deemed responsible for suspected loss of information in the course of ensuring that a malware free environment is maintained. It will also not be deemed liable if anti-malware software plus latest updates have been installed and have failed to prevent a viral infection occurring which results in loss or corruption of data, or loss of any ICT service.

6.10 Additional Security Recommendations (Personal Devices)

There a several simple actions that will ensure a safe environment for personal devices:

- Ensure you device’s Firewall is turned on at all times. This will stop unwanted access to the computer on the Internet (especially at home).
- Ensure that some form of anti-virus and anti-spyware software is running and that it is updated at least on a daily basis
- Ensure that your device is setup to receive operation system updates & check for updates on a weekly basis.

- Only download software from trusted sources. Windows, Mac, iOS & Android devices have ‘App Stores’ that contain pre-screened application that are safe to download. Use these sources when available.
- If the application is not available in an App Store, ensure that any downloaded software is from the vendors site and not another source.

7.0 Email and Messaging Procedure

7.1 Introduction

All email and messaging users (staff and students) are bound by the terms and conditions of the College’s Computer Services Acceptable Use Policy.

Note that “Messaging” includes any form of electronic messaging including instant messaging, text messaging and any form of web messaging service.

7.2 Acceptable use of Email and Messaging

The following guidelines must be adhered to:

- Users may access only their own mailbox and must not use or attempt to access another mailbox. It is not permissible to send e-mail from another College staff or student mailbox unless approval has been granted by both the mailbox owner and the sender’s line manager.
- Users are discouraged from sending large file attachments to individual or multiple mailboxes to either internal or external recipients. “Large” can be defined as anything over 30MB.
- In order to reduce the risk of malware infection, users should not open file attachments of any file type unless:
    - It is a Microsoft Office file (i.e. Word document, Excel spreadsheet) and
    - It is a file that they are expecting to receive or has been sent to them from a known and reputable source.

  Please delete dubious mail messages or check with ITS Department for advice (see Section 7.3 for more information).
- Users must not e-mail or message any illegal, malicious or copyright protected files or information.
- Users are not permitted to use the College email and messaging services as a medium to transmit offensive or abusive material or messages.
- Email should be used for SERC business; teaching or study-related activities provided such activities are legal.
- Email spamming is forbidden. (Spamming is the forwarding on, or sending of unwanted e-mail to other users or groups of users without their prior knowledge or consent). The mailing of multiple users, or multiple mailing groups, or the mailing of one user or mailing group many times is also considered as spamming.
- Phishing e-mails must not be created or forwarded to others. Furthermore, phishing e-mails received that request personal (including passwords or usernames), financial or other confidential or sensitive information should be reported and deleted.

- Each user is responsible for managing the content of their mailbox. There is an expectation that each user will delete processed messages from Mailbox folders. SERC cannot guarantee the integrity and indefinite storage of mailbox information.
- E-mail can be set up and accessed on mobile devices such as mobile phones and tablet computers as long as the devices are secured in accordance with the terms of the Remote Access and Mobile Computing Procedure.
- All messages should be constructed observing acceptable etiquette. (For example, capital letters and large fonts should be avoided.)

7.3 Dealing with Dubious or Suspicious Emails

The most common forms of harmful or nuisance e-mail types are as follows:

- Messages that contain malware. These are e-mail messages which contain attachments that contain malware. The recipient is encouraged or instructed to open the attachment. Once opened, the malware is activated and will infect the recipient's machine and will in many cases attempt to spread to other machine by various means. Some malware can create their own e-mail address or can harvest other e-mail addresses and then send out to other recipients. As the sending e-mail address may well be the e-mail address of someone known to the recipient, they can be duped into opening the attachment.
- Messages that attempt to obtain personal or confidential information, referred to as phishing. These messages try to convince recipients of the necessity to provide personal details such as banking details, user names and passwords. This can lead to loss of information, or to loss of money from bank accounts. There are several variations of this technique beyond basic bulk mailing including:
    - Spear Phishing - fake but genuine looking emails based on intelligence gathered about the target from social media and other publicly available information.
    - Whale Phishing - similar to spear phishing, but specifically targeting upper management and their role in the company.
    - Clone Phishing - the use of a previously sent email used as a template, but with hyperlinks substituted with links that lead to malicious websites. The sender is also impersonated with a similar name & email address in an attempt to fool the target.
- Messages that contain hoax messages. There are messages that try to scare recipients into believing that a harmful virus is circulating and advise the recipient to pass the message on to other friends and colleagues. Messages encouraging recipients to pass on to many other recipients is often referred to as "chain mail".
- Messages that flood many mailboxes (spam). There are messages that are generated with the sole intention of flooding mail servers so as to deny access to mail users. Such messages are referred to as spam.

There are many other forms of messages that circulate containing advertisements and other information which many would regard as "junk" mail. Some would also classify such mail under the category of "spam". The college has systems in place to deal the majority of this content, however, this is not an exact science & some unwanted content will still slip through. Users are therefore asked to be wary of this type of content and to report/delete any content that slips through using MS Outlook 'Report Message' facility.

7.4 Breach of guidelines

Breaches of above guidelines could result in the perpetrator(s) having their e-mail account(s) disabled. Serious offences could result in further disciplinary action being taken. As stated in the Acceptable Use Policy, SERC retains the right to check material stored on computing facilities if it is suspected that the acceptable use policy has been violated.

7.5 Staff and Student Leavers

Final year students will have their mailboxes deleted six months after leaving the college. (Their computer accounts will expire 3 months after the end date of their course).

When a staff member leaves the College, they will have their e-mail accounts disabled for three months and then their mailbox will be deleted.

8.0 Internet Use Procedure

8.1 Introduction

All Internet users (staff and students) are bound by the terms and conditions of the College's Computer Services Acceptable Use Policy. The College uses web filtering software to block out prohibited sites and material. In the event that a user inadvertently access any offensive or sexually explicit material, for example from a link in an email, they should leave that site immediately and inform both their Line Manager/course tutor and the IT & Services Department giving details of the URL visited.

As stated in the SERC Acceptable Use Policy, SERC retains the right to monitor the transmission or storage of material through its computing services if it is suspected that acceptable use has been violated.

8.2 Acceptable Internet Usage

The Internet should be mainly used for business or study related activities.

8.3 Unacceptable Internet Usage

The Internet should not be used for:

- Excessive personal use. (Personal use is permissible during break times).
- On-line gambling.
- On-line share trading.
- Accessing or downloading pornography.
- The obtaining and spreading of malware.
- Downloading or distributing copyright information.
- Downloading of software including games and screensavers.
- Posting confidential College information or information about other employees or students.
- Abusing, harassing or criticising any other staff member, student or third party.
- Circulation of defamatory statements either from within or from outside of the College.
- Deliberate overloading or attempts at the disablement of any ICT service.

- Downloading of large (over 3GB per file) video and audio files unless prior authorisation has been sought.
- The circumvention of College ICT security measures.
- Accessing of chat rooms and social networking sites unless permission has previously been granted by the course tutor and Head of ICT for students and Head of ICT for staff access.
- As a medium for transmission or receipt of abusive or offensive mobile phone text messages.
- Any other activity considered to be illegal or in breach of any College policy or procedure.

Use of internet mail services such as Hotmail, Yahoo etc. should only be used for personal correspondence. Students and staff should use their College e-mail accounts (ending in @serc.ac.uk) for all educational related activities.

8.4 Accessing and use of Social Media and Blogging Web Sites

The College will block access to social media sites for staff and students as a general rule. However, exceptions can be made for particular staff and student groups if it is deemed necessary for business or educational purposes. (See Section 9.0 -

Social Media)

8.5 Reporting of incidents and making a complaint

Any alleged breach of this procedure should be reported in first instance to a staff member's line manager in cases relating to staff.

Any breaches in relation to a student or students, should be reported to the student's course tutor or Deputy Head of School.

In cases where breaches are considered serious, disciplinary action could ensue.

Thirty parties seeking to make a complaint in relation to a breach of this procedure by staff or student(s), should avail of the College's complaints procedure.

9.0 Social Media

9.1 Introduction

Through the responsible use of social media, SERC is committed to safeguarding the confidentiality and reputation of students and staff, and the reputation of the College.

For the purposes of this SOP, social media is defined as any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public or internal forum. This constantly changing area includes (but is not limited to):

- Online social forums such as Twitter, Facebook & LinkedIn.
- Blogs, videos and image-sharing websites such as YouTube & Instagram.
- Messaging technologies such as Skype, WhatsApp, iMessage & Snapchat.
- Dating apps
- Personal web space

These procedures should be followed in relation to any social media used to promote good practice, protect the College and its staff and to promote the effective and innovative use of social media as part of official SERC activities.

Although the College will block access to social media sites for staff and students as a general rule, nothing is intended to restrict or inhibit activities involving social media in accordance with College needs or legitimate academic research.

Staff and students:

- Should not use social media websites to criticise the College, or any staff members, students or third parties.
- Should not use social media websites to abuse, harass staff members, students or any other third parties.
- All staff and students must remember not to post any comment, or image that would bring the College into disrepute, or give cause for a third party to consider taking legal action.
- Must not place information pertaining to, or upload image(s) of College staff or students to any web site without the prior consent being obtained from the staff and student member(s) in question.

9.2 Scope

This guidance applies to:

- All staff employed
- All Students
- Third parties engaged by or on behalf of SERC

It applies to the use of social media for business, whether it is in normal work time or not, on SERC or personal computing facilities and whether posting on social media using personal or work related accounts.

9.3 Breach of Procedure

Any breach of the procedures may lead to disciplinary action being taken against the individual(s) involved in line with SERC Disciplinary Procedures.

The Marketing and IT Services departments must be informed immediately of any breaches of Social Media procedures so that appropriate action can be taken to protect confidential information and limit damage to the reputation of SERC.

9.4 Use of Social Media at Work

Staff may be required to make reasonable and appropriate use of social media as part of their work, where this is an important part of how the College communicates. Staff should be accurate, clear and transparent when creating or altering social media sources of information about SERC.

Procedures for setting up social media for business purposes are set out in Section 9.7.

Staff must be aware at all times that, while contributing to the College's social media activities, they are representing SERC and should use the same safeguards as they would with any other form of communication.

Staff should keep their professional and personal lives separate when using social media. SERC reserves the right to monitor internet usage as per the provisions of the SERC ICT Security Policy & ICT Systems and Services SOP.

When using social media for communicating SERC business, staff must NOT:

- **Bring SERC into disrepute**, for example by:
    - presenting personal views as those of SERC.
    - criticising or arguing with customers, clients, colleagues, students or rivals.
    - making defamatory or libellous comments about individuals or other organisations or groups.
    - posting images without the correct consent, or that are inappropriate, or links to inappropriate content.
    - Edit open access online encyclopaedias such as Wikipedia in a personal capacity whilst at work (the source of the correction will be recorded as the SERC IP address and will appear as if it comes from SERC itself).
- **Breach confidentiality legislation or codes of conduct**, for example by:
    - revealing confidential information owned by SERC.
    - giving away confidential information about an individual (such as a colleague, student, or customer contact) or organisation (such as a rival business).
    - discussing SERC's internal workings (such as future business plans that have not been communicated to the public).
- **Breach copyright**, for example by:
    - using someone else's images or written content without permission.
    - failing to give acknowledgement where permission has been given to reproduce something.
- **Breach data protection legislation**, for example by:
    - disclosing information about an individual without their consent.
    - allowing unauthorised access to the personal data held on a social media account on behalf of SERC.
    - processing personal data in such a way that would breach Data Protection principles.

- **Do anything that could be considered defamatory, discriminatory against, bullying or harassment of, any individual or organisation**, for example by:
    - attacking, insulting, abusing or defaming any students, their family members, staff, SERC or other related professionals.
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief, pregnancy/maternity, marriage and civil partnerships, or age
    - Posting images or videos that are discriminatory or offensive (or links to such content).

9.5 Personal Use of Social Media

Although SERC permits personal use of social media for staff, they are reminded that access to these facilities is a privilege and that social media use shouldn't interfere with their responsibilities during working hours. Student access is currently permitted on a case by case basis, however the principle of privilege and responsibility applies equally to students to whom access has been granted.

While they are not officially acting on behalf of SERC, staff must be aware of the damage to the College if they are recognised as being employed or engaged by SERC.

Any communications that staff make in a personal capacity through social media must not bring SERC into disrepute, breach confidentiality or copyright, breach data protection, or do anything which could be considered defamatory or discriminatory against any individual or organisation.

In relation to personal use of social media, SERC staff must NOT:

- Use SERC email addresses and other official contact details for setting up, or communicating through, social media accounts.
- Identify themselves as SERC employees.
- Publish photographs, videos or any other types of image of SERC students on personal social media.
- Have contact with any SERC student, unless that student is a family member or pre-existing personal friend.
- Have contact with any student's family member if that contact specifically relates to SERC business, is likely to constitute a conflict of interest, or call into question the staff member's objectivity.
- Accept 'friend requests' from students; they should signpost students (during class time) to become 'friends' of one of the official SERC social media sites.
- On leaving SERC service, contact SERC students via personal social media sites. Similarly, current SERC staff must not contact students from any educational establishment they were previously employed at by means of personal social media unless that student is a family member.

Staff should apply caution when inviting or accepting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships if too much personal information is known in the work place.

Staff are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their

own privacy. Staff should keep their passwords confidential, change them often and be careful about what is posted online. It is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

9.6 Social Media Monitoring

The College reserves the right to monitor employees' use of social media on the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- Promote productivity and efficiency;
- Ensure the security of the system and its effective operation;
- Make sure there is no unauthorised use of the College's time;
- Ensure that inappropriate, restricted or blocked websites are not being accessed by employees
- Ensure there is no breach of confidentiality.

The College reserves the right to restrict, deny or remove Internet access, or access to particular social media websites, to or from any employee or student. Abuse or misuse of access may also result disciplinary action.

9.7 Setting up Official SERC Social Media

Advance permission must be obtained from Communications and Marketing before creating any new official SERC social media site to ensure that any new presence is aligned with college strategy. There must be strong pedagogical or business reasons for creating official SERC social media sites to communicate with students or others. Staff should also refer to the Photographs and Video Involving Children and Vulnerable Adults SOP to ensure that student privacy is respected.

To request the set up an official SERC social media site, contact the Marketing Officer (Social Media) to progress the matter.

10.0 Network Management Procedure

10.1 Introduction

The computer network is a fundamental service that provides the infrastructure to enable connectivity between all of the South Eastern Regional College's computing resources. It is vital that such a resource is properly controlled, maintained and managed.

10.2 Purpose

The purpose of this procedure is to clearly delineate responsibility for all aspects of the computer network while at the same time allowing sufficient flexibility to ensure an efficient service can be delivered to the various College Units and Schools

10.3 Definitions

For the purposes of this document, the list below defines specific terminology:

- **Remote Access Devices** - Any equipment capable of establishing a physical network connection with a device or network that is not owned or operated by the College.
- **Network Components** - Includes, but is not limited to: switches, routers, firewalls, interface converters, patch cables and data cabling, wall sockets, wireless access points, remote access devices & servers.
- **Cloud Services** – Includes 3rd party hosted Software as a Service (SaaS), Platform as a Service (PaaS) & Infrastructure as a Service (IaaS) functions.
- **End User Devices** - PCs, Macs, Laptops, Macbooks, Servers, Workstations or other devices that are not performing the function of a Network Component.
- **The College's Computer Network** - All of the Colleges controlled Network Components that are directly or indirectly connected to the external JANET interface (or its replacement).
- **The IT & Services Department** - The body responsible for all activities pertaining to the Computer Network.

10.4 Procedure

The College requires that only authorised persons shall manage and maintain the operation of the computer network.

The IT & Services Department has ownership of all Network Components comprising the Computer Network and will oversee procurement of all Network Components that are to be connected directly or indirectly to the Computer Network.

The IT & Services Department is responsible for the:

- Installation/connection of any and all Network Components to the Computer Network. The IT & Services Department may, at its discretion, delegate specific activities to End User departments to support their activities as efficiently as possible.
- Configuration and management of all Cloud Services & Network Components comprising the Computer Network.
- Management of all network based protocols, e.g. IP addresses, DNS, DHCP, Routing protocols/tables etc.
- Management of all aspects of network security, traffic profiling, traffic prioritisation, authentication and control of access to the Computer Network.
- Performance monitoring and measurement exercises of the network.

- Management of radio frequency separation on all College sites, for all wireless Network Components irrespective of usage.
- Management of the capital and revenue budget for the Computer Network.
- Disaster recovery of the network.

10.5 Update of Systems

Nearly all network components in a modern network have some sort of operating system. The regular update of these systems is an important task in ensuring a secure network. Where possible:

- Hardware devices such as switches & routers should be kept up to date with the relevant security firmware when release by the vendor.
- Servers/Workstations should install monthly security update within 2 weeks of release.
- Application that run on servers or workstations should be updated at minimum when vulnerabilities are published.
- Where it is not possible to update a device, operating system or application, an assessment should take place in relation to the risk and if possible, action taken to reduce or remove the risk. This may take the form of a configuration change or the removal of the device from the network.
- The College's cloud based threat management tools provide an inventory of software and vilnerbilities.

10.6 Fault Management & End User Support

The IT & Services Department will operate a Fault Reporting facility for the logging of all faults and problems with the Computer Network. All faults requiring the attention of the IT & Services Department must be logged. The IT & Services Department will work closely with nominated representatives of End User Departments to support the resolution of problems as efficiently as possible.

Remote support tools will be used by IT & Services staff in order to provide end user support. Where possible, permission should be obtained from the end user before connection to the remote device takes place. Remote tools will not be used for "spying" unless there is due cause to suspect inappropriate use by an end user.

There will be no monitoring or recording of the data content of packets traversing the Computer Network without the explicit permission of the IT & Services Department

10.7 Remote Access

Requests for VPN (Virtual Private Network) access to the College Network for College staff must be approved by the Departmental Head and the Head of Networks or Chief Technology Officer.

The College will provide remote access for staff and students to the College Intranet. It is incumbent upon each remote user to ensure that their remote devices are up to date in relation to operating system updates & protected by an up to date anti-malware solution.

10.8 Third Parties

Third parties are expected to adhere to the relevant guidance in the colleges Supplier Information Security Requirements document. New suppliers should complete a Supplier Security Assessment Questionnaire before gaining access to college systems.

Requests for remote access to the College network or any College ICT System by third parties must be addressed to the Head of networks or Chief Technology Officer for approval.

Upon approval, a time limited user account will be created with the required access and an agreed method of secure connection e.g. VPN will be provisioned.

When the third party requires access to the College network, the third party must request access from a member of the College network management team by emailing networkmanagers@serc.ac.uk giving details of reason(s) for requiring access, the identity of the party or person accessing the network and the estimated duration of access. Access will then be granted on a time limited basis.

If an extension of access is required, the third party should email networkmanagers@serc.ac.uk with the request. When all work has been completed, confirmation of work carried out must be provided by the third party.

10.9 Computer Accounts for Staff and Students

All Staff and students will be given an account to log on to PCs/Macs for purposes of accessing e-mail, file storage, internet/intranet services.

Accounts will be set to expire upon the staff member leaving, or at the end of the course + 3 months for a student. Accounts for staff on temporary and part time lecturing contracts will be set to expire at the same date as their contract end date. Part time lecturing staff on a waiting list will not have active accounts until they are engaged in teaching and are given a contract.

11.0 Password Procedure

11.1 Introduction

Passwords are an important aspect of computer security. They form the front-line protection for user's accounts. A poorly chosen password may result in the compromise of the College's entire network. As such, all staff, students and contractors that have access to any computer system at any College Centre are responsible for taking the appropriate steps to select and secure their password.

11.2 Purpose

The purpose of this procedure is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

11.3 Scope

The scope of this procedure includes all staff, students and contractors who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any SERC Centre or Campus.

11.4 Procedures for College Systems

- All system-level passwords (e.g. root, enable, Windows server administration, application administration accounts etc.) must be changed on at least a yearly basis.
- All user-level passwords must be changed at least every six months.
- Passwords should not be disclosed in emails, phone calls, questionnaires, or verbally via a third party.
- Where SNMP is used, the community strings must be defined as something other than the standard "public", "private" and "system" and must be different from the password used to log in interactively.
- All system-level and user-level passwords must conform to the guidelines described below.

11.5 General Password Guidelines

The college requires the use of complex & strong passwords. The following characteristics are required:

- Passwords need to be at least 10 characters long and no longer than 127 characters
- Passwords should not contain either your username or your forename & surname
- The space character can be used in a password, but his is not a requirement
- Passwords have to contain characters from three of the following categories
    - Uppercase letters (A through Z)
    - Lowercase letters (a through z)
    - Numbers (0 through 9)
    - Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
      Note: Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting.

Users are asked to consider a ‘passphrase’ instead of a password. Passphrases can be a sentence, song title or other phrase that is easy to remember. Some example passphrases would be:

- The 0nly Way 1s Up!
- H0ld the d00r!
- My fav0rite c0l0ur is Red

Passwords should never be written down or stored on-line as clear text. Users should also avoid common usage words such as:

- Your forename, surname, name of family, pets, friends, co-workers, course title etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- SERC, South Eastern Regional College.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like 1234567, abcdefghi, qwertyuiop etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g. password1).

11.6 Password Protection Standards

Staff & students are strongly advised not to use the same password for SERC accounts as they may use for other non SERC accounts such as personal e-mail accounts, Banking accounts, PIN numbers, or any other account. Where possible, staff & students are also advised **not** to use the same password for various SERC systems. For example, select one password for the Agresso system and another password for the network log in. The exception is when Federated Identity or Single Sign On (SSO) has been configured, discussed in section 11.7.

The college requires that passwords are changed every 6 months. This change is enforced automatically by the system.

Staff & students should **not** share SERC passwords with anyone, including classmates, administrative assistants or line managers. All passwords are to be treated as sensitive confidential SERC information. If someone demands a password, refer them to this document or have them call someone in the IT & Services department.

Staff or Students should be advised to never disclose their password in response to an email or phone call purporting to be from the IT department. The IT & Services department **should not and will not** ask an end user password to divulge their password.

For the avoidance of doubt, it is not permissible to:

- Reveal the password over the telephone to anyone.
- Reveal a password in a single e-mail message.
- Reveal a password to a manager or lecturer.
- Reveal a password to co-workers for their use while you are on holiday.
- Talk about a password in front of others.
- Hint at the format of a password.

- Reveal a password on questionnaires or security forums.
- Share a password with family members.
- Write passwords down and store them anywhere in your office.
- Store passwords in a file or on ANY device without encryption.
- Use the “Remember Password” feature of applications on devices, unless the device is password protected and uses encrypted storage.

The single exception to the above guidance applies only to students with specific physical and/or learning needs. In this scenario, a support worker may, with the consent of the student, be allowed to hold knowledge of a student password for the purposes of assisting the student with their study.

If you suspect your password has been compromised, report the incident to the IT & Services Department and change your password immediately.

11.7 Federated Identity & SSO

Some college systems and 3rd party websites are integrated with the colleges Identity Provider (IdP) in a configuration knows as federated identity. This allows a SERC account (including password) to be used to login to a non SERC service, such as a website. This method is considered more secure as the foreign website does not hold the password for the user. These configurations are vetted & preconfigured by the IT & Services Department.

Only the IT & Services Department can setup new federation partnerships. In order to add a new federated partnership, staff & students should contact the IT & Services Department with details and a justification for the service they wish to add. The service must be evaluated, authorised and configured by the IT & Services Department to ensure it meets minimal security standards. All requests must be approved by the Chief Technology Officer or Head of Networks.

SSO configurations should only be used on devices managed by the IT & Services Department. It is no permissible to have SSO enabled on a device that does not have a lockout time less that 5 minutes. Additionally, SSO should not be used for services such as HR, Finance or Student Records.

11.8 Additional Security Measures (2FA/MFA)

Two/Multi Factor Authentication is available to all staff & students. Passwords are sufficient for staff and students when logging into college managed devices, however when using non-managed devices, the following restrictions will apply:

- Staff Access to college computing facilities will be restricted to college managed devices unless 2FA/MFA has been enabled on the user account.
- In addition, even with 2FA/MFA enabled, staff login will be restricted to EU countries. This restriction will be relaxed for a time limited duration for individual staff on request for travel outside EU borders.
- Student Access to college computing facilities using username & password will be restricted to the UK/Ireland unless 2FA/MFA has been enabled on the user account.

Two-Step Verification can be setup from the following link: https://aka.ms/setupsecurityinfo

11.9 Changing/Resetting Passwords

All IT & Services Staff can reset any other College staff or student member's password, however it is not possible for IT & Services staff to reset other IT & Services staff passwords unless they are in the role of network manager or above.

The preferred method of changing a password i.e. when the user knows their existing password, is using a College PC/Mac or from the sign-in screen when logging in remotely.

Where a user has forgotten their password, the preferred method of resetting a password is via self-service password reset. This can done using a college PC, clicking the 'Reset Password' link on the login screen and following the instructions. When accessing the system remotely, this can be done using the 'Forgot Password' link on the log on screen. Note that in order to use self-service password reset, a mobile phone is required.

Self-service password reset can be setup from the following link:
https://aka.ms/setupsecurityinfo

Where self-service password has not been configured, all teaching staff can reset a student's password by using the 'Student Lockout Wizard' which is available on the College Staff Intranet. However, if this method is employed, teaching staff must permit the student to enter the password. Staff should not enter a student's password or request that a student disclose their password. Activity on this system is logged and misuse may result in disciplinary action.

When resetting staff accounts, IT & Services Staff should ensure that the requestor is who they say they are. In most cases, suitable ID should be produced in person before the password can be reset. Remote password reset is permissible, but IT & Services Staff should be assured beyond doubt that the requestor is who they say they are.

Students should not have their password reset either in person, via e-mail or telephone unless the IT & Services Staff member can have strong assurance of authenticity of the person requesting. The minimum requirement for establishing authenticity is to obtain several of the following pieces of information:

- photographic Identification (Student Card, Drivers Licence)
- an identity verification by another member of staff
- student/staff number
- an address or postcode
- in case of student request, the course of study
- in the case of student, the name of another person in the same class or tutor name

If there is any uncertainty, IT & Services Staff are instructed to refuse the request in a respectful manner, explain the importance of security and ask the user to return and present the required evidence. Staff & students are expected to be courteous when a password reset is refused, and aggressive or threatening behaviour will not be tolerated. Feedback or complaints should be made to the Chief Technology Officer in writing via email or letter.

Upon establishment of authenticity, the password can be disclosed as long as:

- A temporary password is broken into 2 parts and transmitted in two separate e-mails.
- A temporary password is agreed in a phone call.

- I both of the above scenarios, the “User must change password at next login” attribute must be set by the ICT Staff member on the user account, forcing the end user to choose a new password that only they know.

11.10 Enforcement

College accounts are monitored against known data breaches. If an account is found in known breach lists and the password is the same as the current user’s password, the password will be reset immediately and a either a self-service password reset will be required or the user will need to contact college IT in order to reset.

College accounts are also monitored for suspicious activity. In the event that an account displays suspicious activity, the password will be reset immediately and a either a self-service password reset will be required or the user will need to contact college IT in order to reset.

Password “cracking” or guessing may also be performed on a periodic or random basis by IT & Services staff. If a password is guessed or “cracked”, the password will be reset immediately and a either a self-service password reset will be required or the user will need to contact college IT in order to reset.

It is prohibited for non IT & Services staff or students to attempt to guess or “crack” the password of another user. Any member of staff or student found to have violated this procedure may be subject appropriate disciplinary action.

12.0 ICT Security Controls and Incident Procedure

12.1 Introduction

This procedure outlines responsibilities, structures, controls and the process for reporting ICT systems security incidents. It applies primarily to staff of the College. However, all users of College information systems are expected to abide by this and all procedures related to ICT systems security.

With increasing reliance on electronic information comes a corresponding concern for the security of that information, particularly with mobile technologies such as wireless and 4G.

Since neither the systems, technologies nor those who operate them can ever be totally reliable, the College must be able to react promptly and appropriately to any security incident, and to restore its information systems to their normal operational state in an acceptable period of time. One of the most fundamental aspects of information security is an information security procedure which amongst other things, defines responsibilities for information security and identifies the needs for security controls.

12.2 Requirements for Security Controls

A number of security controls are in place to permit the proper management of information security. Key controls are as follows:

Corporate Management Control

The Information & Cyber Security Committee (ICSC) is the principal management structure for overseeing key aspects of corporate ICT systems security. This group will have responsibility for:

- Policy and guideline formulation on security.
- Provision of guidance and direction to the College's Governing Body and College Management team on security issues.
- Ensuring that there is management support for security initiatives.
- Managing security incidents.
- Co-ordinating implementation of corporate security measures.
- Initiate security audits and ICT risk assessments.
- Identifying risks to ICT systems and services and ensuring that they are recorded on the College's risk register for presentation to the Risk Management Group.

The group will play a key part in informing and advising all users of ICT systems within the College of major security policy decisions and plans for implementation. Should a security incident occur, the ICSC will have authority to scrutinize any evidence pertaining to the incident.

System Management Controls

Data Owners (System Managers), for all major College systems, will have primary responsibility for ensuring that:

- Appropriate security measures are in place to safeguard services and data.
- Key stakeholders are informed and abide by security policies and procedures for each system.

- Ensure that breaches in security are reported to the ICSC.

System Controls

Each system itself is required to have in-built and/or configured security controls to guarantee the integrity of data and services. Controls include:

- Access levels (See also 5.0 Access Control Procedure)
- Password controls. (See also 11.0 Password Procedure)
- Authentication measures (where appropriate)
- Data encryption (where appropriate, 14.0 Data Management Procedure)
- Backup (See also 14.0 Data Management Procedure)

Physical Controls

Logical controls against information only provide part of a security & integrity framework. Information is still at risk if key systems a physically vulnerable to tampering or theft. Physical controls should therefore include:

- Secured areas for location of key ICT items.
- Doors to any ICT device will be locked whilst the area is unattended.
- Authorised personnel only will be permitted only to restricted areas such as communication and server rooms.

12.3 Security - Good Practice Guidelines

The following is a non-exhaustive list of Security Good Practice.

DO

- Lock workstations & devices whilst left unattended.
- Report suspicious behaviour or persons acting suspiciously.
- Ensure college owned devices connect to the College network on a weekly basis for anti-malware and operating system updates.
- Ensure your personal devices have up-to-date anti-malware software installed, you firewall is enabled and that you check for operating system updates on a weekly basis.
- Change your password if you have any concerns.
- Enable 2FA/MFA

Never

- Disclose your password to anyone.
- Leave rooms unlocked that contain ICT equipment.
- Use someone else's password.
- Open unexpected e-mail message attachments.

- Accept as genuine all e-mail content.
- Spread chain mail (e-mail that you are invited to pass on to others).
- Leave passwords written for viewing by others.
- Use names of family members as passwords.
- Supply personal or business information to any third party unless authorised to do so.
- Store any personal or business data on local drives of Desktop, Laptop computers, or Tablet & Phone devices unless the drives/storage is encrypted.
- Attach any device to the College network unless authorised to do so.

12.4 Procedure for reporting a security incident or security vulnerability

In the event of an incident, staff or students should:

- If the issue is raised by a student, the incident should be reported to a member of staff.
- Staff members should contact the appropriate College Data Owner & either the Chief Technology Officer or Head of Networks, directly via email/phone or indirectly eg, via the college fault log or a local member of the ITS team.
- In conjunction with the Data Owner, complete an incident report (Appendix 3)
- Remedial action to be taken by the Data Owner (where possible) and ICSC to be informed.
- In such cases where immediate remedial action cannot be taken to fully address the issue, a contingency arrangement must be implemented by the Data Owner in agreement with the Chief Technology Officer to reduce the risk of a further security incident occurring. This arrangement will be in force until a permanent solution is implemented.

12.5 Responsibilities for Information Security

Whilst all users of College information systems have a responsibility to some degree of ensuring that security is not compromised, overall management responsibility for security of College ICT Systems rests with the Chief Technology Officer and the ICSC. Each Data Owner will have specific management responsibilities for their respective ICT information systems. Their key responsibilities are:

- Remove user accounts of users that no longer require access to the data or system.
- Ensure passwords for users are changed regularly.
- Conduct security audits.
- Ensure backups have taken place.
- Conduct regular risk assessments.
- Retain accurate system administration information and store such information securely – (i.e. user names, access granted).
- Report unusual system activity (poor performance, unreliable or unexpected data results).

12.6 Links with other bodies

The College will retain links with other bodies such as JANET(UK) with regards to information security. Internally, the ICSC will liaise closely with Heads of School and Heads of Units in terms of identifying significant ICT-related risks

12.7 Responsibility

CMT, through the ICSC, will be responsible for ensuring that all ICT Systems users are:

- Made aware of the content contained in the security policy and associated policies or procedures.
- Ensure that all staff receive training on the procedure and general security.
- Ensure that policy and procedure revisions and updates are communicated to all users.

12.8 Further Information

More information is available on the Information Systems Incident Management Policy.

13.0 Software Licensing Management Procedure

13.1 Introduction

The College is committed to ensuring that all commercial software applications installed on any of its ICT equipment items are appropriately licensed in accordance with numbers of users who require access. This procedure document outlines the main procedures and controls in place to ensure that licensing regulations are not violated.

13.2 Access

In order to prevent installation of unlicensed software, only IT & Services staff have the necessary access to install software.

Access is granted to the following:

- PCs, laptops, Macs and MacBooks – all IT & Services Staff – (depending upon the method – see Section 13.3. Method of Installation).
- Servers – Senior IT & Services staff only.
- Apple Macs – The technical support staff who work for the Schools of Computing and Media and the School of Performing Arts.

13.3 Method of Installation

There are two main methods of software installation:

- Deployment – Only IT & Services staff are permitted to deploy or authorise deployment of packaged software.
- Manual Installation – Only IT & Services Staff are permitted to install software manually. Regardless of method type. Installations can only take place if sufficient software licences have been procured. Approval for installation must be obtained from the Chief Technology Officer.

(Software Installation Procedure provides details for IT & Services staff on installation of software)

13.4 Authorisation

The procedure for authorising software installation is as follows:

- Request for software installation to be addressed to the Unit Head or Curriculum Head of School for approval.
- If approval in previous step is granted, then the request is to be forwarded to Chief Technology Officer by the Departmental Head or Head of School for licensing confirmation.
- Installation authorisation to be granted by Chief Technology Officer to appropriate ICT technical staff.

13.5 Control

All staff and students (other than groupings stated above in Section 13.2) do not have the necessary permissions to install software on PCs and laptops.

All staff and students are compelled to adhere to the College's Acceptable Use Policy which forbids use of unlicensed or unauthorised software.

13.6 Procurement and Recording

Procurement of application software must be approved out by the Chief Technology Officer.

14.0 Data Management Procedure

14.1 Introduction

An influx of new technologies, greater dependence on electronic data and changing working practices such as hot-desking, have contributed to make it more difficult for an organisation to manage data. The purpose of the procedure is to provide guidance on managing corporate data within the College. The procedure will in most part apply to College staff but will also have an impact on students on terms of management of their course related data.

14.2 Classification of data types

"Data" will include any type of information stored on any electronic storage medium, including files, documents, e-mail, database records. Broadly speaking, all data used in SERC maps to the Cabinet Office's Government Security Classification level of **OFFICIAL**. Internally, SERC uses a further set of sub classifications. These are:

- General
- Confidential
- Sensitive

'General' data can be defined as:

- Business data that is intended for public consumption or that may be shared with external partners as required. Some examples include:
    - the internal telephone directory.
    - organizational charts.
    - internal SOPs/Policies/standards, and most internal communication.
- Documentation relating to teaching activity such as schemes of work or lesson plans or other resources.
- Business data that is specifically prepared and approved for public consumption. Some examples include:
    - College Prospectuses or other marketing materials.
    - Website content.
    - Minutes of governing body meetings.
    - Photographic images made public with an individual's consent.
- Any other stored data which does not fall into the 'Confidential' & 'Sensitive' categories.

'Confidential' data can be defined as:

- Any information containing names and including any, or all of the following:
    - Dates of birth.
    - Addresses & postcodes.
    - Photographic images.
- Prospective & current student contact, registration and attendance details.

- Exam papers.
- CCTV footage.
- Sensitive business data that could cause damage to the business if shared with unauthorized people.
- Any information that would offer competitive advantage to other colleges, or competitors.
- Any information that could mean loss of business, revenue or reputation to the College should that information be available outside of the College domain.

'Sensitive' data can be defined as:

- Documents containing GDPR Special Category information about the following subject matter:
    - Racial or ethnic origin.
    - Political opinions.
    - Religious or philosophical beliefs.
    - Trade union membership.
    - Genetic data.
    - Biometric data for the purpose of uniquely identifying a natural person.
    - Data concerning physical & mental health.
    - Data concerning a natural person's sex life or sexual orientation.
- Financial details such as banking details, payroll history or national insurance numbers.
- Passport numbers.
- Details surrounding investigative activity in relation to disciplinary, grievance, harassment or criminal proceedings.
- Any security information such as system passwords, user account details or security procedures & protocols.

14.3 Management of Electronic Data – Confidential & Sensitive classifications

The following guidance is considered by the college to be best practice for all information classifications, however all data classified as Confidential or Sensitive must be treated in accordance with this guidance.

<u>Storage and Transmission of Data</u>

- Data must be stored securely on College approved storage media such as College server file shares, College-provisioned Office 365 Groups/TeamSite or Office 365 OneDrive.
- The use of removable storage devices (e.g. USB keys, removable hard drives) is strongly discouraged. Unless offline access is required, Office 365 Groups/TeamSites or Office 365 OneDrive is the preferred facility for storage.
- Any removable storage device must be encrypted, password protected and require the entry of a password to unencrypt. Where possible/supported, AES 256-bit strength

encryption is preferred, however the general rule is that any encryption is better than none. Windows users may use the 'BitLocker-To-Go' feature whilst MacOS Users may use the 'FileVault' feature.

- Data classified as General, Confidential or Sensitive must not be stored on any external hosted service such as Dropbox, Google Drive or any other similar storage service. The only approved external hosted storage service is Office 365, specifically TeamSite's, Groups & OneDrive. (This has the Government G-Cloud approval for storage for general, confidential and sensitive information).
- Copies of data classified as General can be taken to facilitate remote, or off-site working (e.g. lesson material), for use in a facility with no internet connection.
- Copies of data classified as Sensitive or Confidential must only be taken and transported by portable media as long as:
    - Approval has been sought from Head of School, Unit Head or Director of the specific department or unit.
    - That the method of transportation is deemed secure. Sensitive or Confidential data **must** be transported in encrypted media such as encrypted USB pens, or on encrypted hard drives, or on College-owned laptops that have encrypted hard drives, or any other approved secure media.
    - Great care is taken not to lose or mislay the storage device.
- Where data is to be transmitted over the internet, a secure means of transmission must be used. This should be using a College approved encryption algorithm such as TLS encryption of Web Browser traffic or the use of VPN's. If in doubt, advice should be sought from the IT & Services department.
- Data classified as Sensitive or Confidential must not be transmitted by unencrypted e-mail messages, instant messaging or any other insecure means or media. Where possible, data should be saved to an Office 365 Group/TeamSites or Office 365 OneDrive and shared with the recipient. In addition, Azure Information Protection may be used to securely transmit data.
- It is not permissible to store data classified as General, Sensitive or Confidential on:
    - Personally owned devices such as PCs, laptops, MacBooks, tablets or mobile phones unless they are enrolled in the colleges Mobile Device Management Platform (MDM).
    - Any storage medium, (personal or College provided), if that has not been encrypted. This includes memory sticks, hard drives, camera cards, DVDs and any other storage media

Retention of data storage

- The College will retain data records in accordance with statutory obligations.
- The College will remove mailboxes and data created by students as part of their course 6 months after the conclusion of the course. Students wishing to retain any of their course work may do so before finishing their course.
- Accounts will be set to expire upon the staff member leaving, or at the end of the course + 3 months for a student. Accounts for staff on temporary and part time lecturing contracts will be set to expire at the same date as their contract end date.
- Staff who are leaving College employment are advised to clear out their personal storage and mailboxes before their last day of employment. Staff should pass on

information that could still be required by the College to their Line Manager. This could include exam results, course work or financial or business information.

- Upon receipt of notification from the Human Resources department of staff having ceased employment, staff network login accounts will be disabled & the password will be changed. All data and mailbox contents stored against a disabled account will be deleted after a six-month period.
- The College will not be responsible for loss of data created by staff members or students upon their ceasing their course of study or employment with the College.

Backup

- The College will endeavour to backup and store all corporate data on and off-site. The College backup procedures must be adhered to in performing data backups.
- Where possible, data records, files and documents should be updated on-line or directly to network drives so that the reside in backups in the event of an emergency.
- Offline copies of data taken and updated by staff/students must be uploaded to the appropriate storage area to ensure that the revised content is backed up.
- Where the corporate storage system is capable, version control measures must be enabled.

Data Recovery and Restoration

In the event of data loss or corruption from the College file storage, the following steps can be taken to restore:

- By utilising Shadow Copy for file shares, e.g. M: Drive. If a folder or file has been lost or corrupted it can be restored by right-clicking the file or folder in question and then selecting the “Restore from Previous Version” option.
- By using the version history/ransomware protection features of files/folders in Office 365 Groups/TeamSites or Office 365 OneDrive.
- By contacting the IT & Services Section or Data Owner in order to restore from the last disk backup

Remote Access

Accessing College information systems from a remote location such as a place of employment or from home is permitted as long as:

- The device is enrolled in the colleges Mobile Device Management Platform (MDM).
- The device used is secured with the latest anti-malware software and that virus definitions are continually kept updated.
- Passwords are not disclosed to third parties and that third parties are not permitted to access College services using the staff or student’s member account.
- Staff/students log out on completion of the access to College ICT systems.

Further details can be obtained from the “Remote Access and Mobile Computing Procedure”.

14.4 Return, Disposal and Transfer of Physical Media

College data may reside various forms of physical media. The college has a responsibility to securely dispose of this media and to comply with it's obligations under the Waste Electrical and Electronic Equipment recycling (WEEE) Regulations 2013. This media includes:

- CD/DVDs
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers
- Embedded Microchips (including ID Cards and Mobile Phone SIM Cards)
- Digital Photo/Video Cameras
- Backup Cassettes

Return of media

All corporately owned storage devices or medium issued to end users must be returned to the nearest ICT office for secure disposal when no longer required. Damaged or faulty removable media devices must not be used. It is the duty of all users to return any removable media that may be damaged to ensure the safe disposal of the device, regardless of its physical state.

Transfer of Media

Whilst in transit, data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password protection must be applied to either the entire storage device e.g. disk level encryption or to the individual data files unless there is no risk to the college, other organisations or individuals from the data being lost whilst in transit or storage.

Disposal of media

When physical media is deemed to have reached the end of its useful life, the media/devices must be securely wiped to ensure that no sensitive data is retrievable. Secure erasure is deemed as 3 consecutive full disk formatting operations for unencrypted medium or 1 formatting operation and the destruction of the recovery key for an encrypted medium. This activity must be performed by trained personnel. Once securely erased, media must be disposed of as per WEEE regulation.

The table below outlines the required actions:

Medium	Disposal Method
CD/DVDs	Physical Destruction
External Hard Drives (Mechanical & SSD) *	Secure Erasure or Physical Destruction
USB Memory Sticks (also known as pen drives or flash drives) *	Secure Erasure or Physical Destruction
Media Card Readers	Secure Erasure or Physical Destruction

Embedded Microchips (including ID Cards and Mobile Phone SIM Cards) *	Physical Destruction
Digital Photo/Video Cameras *	Secure Erasure or Physical Destruction
Backup Cassettes	Physical Destruction

* Note that physical destruction is required if the device is damaged.

14.5 Security

All corporate data must be stored on secured College servers with the appropriate authorisation for access granted by the relevant System Manager.

User logins and passwords

Each user of a College system must be allocated a user account and password. Staff accounts can only be setup upon notification from Human Resources Department that all appropriate checks and controls have been completed (this includes signing of Acceptable Use Policy). Passwords must also comply with the College Password Procedure (Section 11.0).

Version Control

Manipulation of copied data incurs risk of multiple partially updated copies of the source documents or files. On-line editing on a single file greatly reduces the risk of multiple copies of partially edited/out-dated documents. However, in instances where on-line editing isn't possible, each edited document should have a date of revision and author name added to the document footer. Reference should also be made to the "Remote Access and Mobile Computing Procedure" to ensure the security of the data.

Malware Prevention

All College servers and desktops will be updated with the latest anti-malware definitions. Only devices with latest anti-malware software are permitted to be used for processing of College data. (Please refer to section 6.0 Anti-Malware procedure for further details on virus control)

14.6 Asset and Inventory Management

All devices used by staff (asset and inventory) such as PCs, laptops, MacBooks, Macs and servers must be data wiped prior to disposal. Data wiping includes removal of all data and software from the device(s). The required process is outlined in section 14.4 (Return, Disposal and Transfer of Physical Media).

14.7 Access to Data

The college has a number of repositories used to store business information. Access to all areas must be controlled using Access Control Lists (ACLs).

Departmental File Shares & Office 365 Groups/TeamSites

Requests for access to above should be made via the Service Desk App and ought to be accompanied with approval from the Head of School/Unit, or Deputy Head of School or Deputy Head of Unit, via e-mail message, indicating the name(s) of staff members and the level of access to be granted (i.e. read access, read and write access).

Requests for access to departmental file shares & Office 365 Groups/TeamSites will be processed by the IT & Services Team.

Access another user's personal drive, Office 365 OneDrive or mailbox

Every staff member/student has their own personal drives and mailboxes. Only that individual has the right to access their own personal drive and mailbox. The following are the only exceptions in terms of other rights to access:

- There is suspicion that inappropriate material is being stored. In such cases, either the Head of School/Head of Unit will consult with the Chief Technology Officer as regards arranging to access the drive/mailbox. The access must be witnessed by the Head of School/Head of Unit and by Chief Technology Officer or a senior member of the IT & Services department (Band 5 or above).
- A staff member is on extended period of absence due to illness or annual leave. Access to the staff drive/mailbox will be granted in urgent cases only if the request is made by the Head of School/Head of Unit indicating the reasons for requiring access to the Chief Technology Officer and only if the staff member in question has given prior approval in writing (e-mail will suffice) to the Head of School/Head of Unit and copied to Chief Technology Officer.
    - The access will only be for a duration long enough to obtain the necessary information and whilst witnessed as stated above.
    - Browsing of the personal drive or mailbox for information other than the required information is forbidden.
    - Once the required information has been located, the access will be removed. The required information is not to be copied or forwarded on, unless the staff member has authorised that.
- If for various reasons, the matter is regarded as most urgent and the staff member's approval cannot be obtained, the matter must be referred to the Chief Human Resources Officer for deliberation.
- Members of the IT & Services Department are not permitted to request access, or to access any other staff member's personal drive or mailbox without the above process being followed.
- A file or folder has been shared by the owner with another user using the Office 365 OneDrive 'Share' feature.

Requests to access personal data on any information system or store

Access requests must be made to the System Manager and Data Owner and must comply with procedures devised for compliance with data protection.

14.8 Discovery of inappropriate data, files, images

Discovery of data, images regarded as inappropriate includes the following:

- Copyright protected files or images
- Images regarded as pornographic, obscene
- Unlicensed software
- Software or utilities regarded as hacking, sniffing, or that can be used in any way to circumvent network or system controls or security.

(The above listing is not to be regarded as definitive)

Discovery of any above must be reported immediately to the IT & Services department so that removal of the items can be arranged. However, discovery of any material which has constituted a criminal offence or could form part of a criminal investigation must be reported to the Chief Technology Officer, the Director of Curriculum & Information Services (or a member of the SMT in the Director of Curriculum & Information Services absence), who will then contact the PSNI.

14.9 Disclosure of Information

It is not permissible for any College information asset, either written or contained in any College information system, to be disclosed to college staff or students who do not have a valid business reason for access. The same rule also applies to 3rd parties, with additional contractual & Data Protection requirements such as security assurances, privacy impact assessments and data sharing agreements being required as a pre-requisite.

This use of college information assets for the purpose of offering a competitive advantage to any third party is prohibited unless authorised by the CMT and, if necessary, the relevant Data Subject/s consent has been given. It is also not permissible for any staff member to use any college information assets to further any independent or private business venture.

Information disclosure must be authorised in line with the conditions outlined in the College Data Protection Policy. In the event that a disclosure exercise involves the removal of college equipment for use/inspection by a 3rd party, e.g Laptops or Servers during a Police investigation, a record of the asset must kept on the college asset register. This should include the details of the individual/organisation taking ownership of the device, contact details, addresses, any known and potential datasets/types and the reason for removal.

Staff are also reminded that, in relation to the accidental release of information, that they have a duty to report and, if possible, prevent any further disclosure of information to other unauthorised staff or 3rd parties.

14.10 Good Practice Guide on Data Management and ICT Security

Personal data is stored by the College in both paper and electronic format. The College must ensure that personal data relating to students, employees and visitors is treated with appropriate security measures by all who handle it. Loss of personal data carries a

substantial risk of causing harm/inconvenience to the data subject and reputational damage to the College

Article 5.1 (f) of GDPR states personal data shall be:

"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

With the majority of information now being digitally recorded, transmitted and stored, it is vital that proper security measures, both technical and non-technical are in place to safeguard College information from loss or theft.

The following good practice guidance may be used as reference materials for end users:

Password Security

Always…

- **Create strong passwords which are easy for you to remember and impossible for someone else to guess.**
- **Follow the General Password Construction Guidelines in Section 11.5 of this SOP**
- **Change password at regular intervals (the college enforces changes every 6 months)**
- **Use Two-step Verification if available**

Never…

- **Use birthdays, addresses, family names, pet names etc….**
- **Disclose your password to anyone, even other members of staff.**
- **Write your password down or save it on a word document.**
- **Select 'yes' if a system asks if you want it to remember your password.**
- **Disclose your password in response to an email purporting to be from the IT department. They will NEVER ask for your password!**

Data & Information Security

Always…

- **Store general/confidential/sensitive information on secure College storage systems i.e. Office 365 Groups/TeamSite or Office 365 OneDrive**
- **Lock your PC/Mac whilst unattended – 'Ctrl + Alt + Del' + "Lock this computer".**
- **Lock classrooms & office doors once everyone has left.**
- **Ensure your personally owned device (PC, mac, tablet, laptop/MacBook) is password protected and has up to date anti-malware software installed.**
- **Have at least a lock password on mobile phones with access to email.**
- **Report any suspicious activity to the IT & Services department e.g. people loitering around equipment.**

- **Bring College provided laptops/MacBook on a weekly basis into the College and ensure that they are connected to the College network for application of essential security updates.**

Never…

- **Store general/confidential/sensitive information on an unsecured mobile device such as a USB pen, personal or third party PC, Mac, laptop, MacBook, Mobile Phone, tablet or external hard drives.**
- **Store general/confidential/sensitive information on a third party storage servie such as Google Docs, Dropbox, Evernote – we cannot guarantee their security. The exception to this will be Office 365 OneDrive.**
- **Use your personal email account for SERC related business - we cannot guarantee their security.**
- **Allow anyone to use your PC/Mac, MacBook, laptop or tablet whilst you are logged in – you are responsible for processing carried out under your name.**
- **Provide personal details of yourself or others to unauthorised third parties.**
- **Respond to web links requesting personal details of yourself or others.**
- **Do not have liquids close to your device in case of spillage.**

Security of College Handheld & Portable Electronic Storage Devices

Always…

- **Guard your mobile device (i.e. mobile phone, laptop, MacBook, tablet) as you would do with your purse, wallet, passport.**
- **Wipe all data from the device before disposing of it.**
- **Report any loss of mobile device to the IT department and change your SERC password as soon as possible.**
- **Turn off Bluetooth when not required to prevent data transfer.**

Never…

- **Leave your device in your car where is it visible to passers-by.**

Photocopiers & Scanners

Always…

- **Store printouts securely e.g. a lockable drawer.**
- **Shred hardcopy personal data which is no longer of use or dispose of in a confidential waste bag.**

Never…

- **Leave the original copy in the photocopier/scanner – always remove it once copying is complete.**
- **Leave copies of personal data where it can be accessed or viewed by other people e.g. staff rooms, unmanned office desks, reception areas, class rooms.**

Remember

It is the responsibility of all staff and third parties authorised who access the College's personal datasets to ensure that data, whether held electronically or manually, is kept securely and not disclosed unlawfully in accordance with the College's Data Protection Policy and the Data Protection Act (2018)/GDPR. Unauthorised disclosure or data loss will usually be treated as a disciplinary matter, and could be considered as constituting gross misconduct with, in some cases, access to facilities withdrawn or even criminal prosecution.

Should personal data be lost or disclosed to unauthorised personnel, the College is obliged to conduct an investigation into the surrounding circumstances and report the incident to the Information Commissioners Office who may in turn issue a monetary penalty notice up to 4% of global annual turnover for serious breaches of the Data Protection Act (2018)/GDPR.

15.0 Remote Access and Mobile Computing Procedure (including BYOD)

15.1 Introduction

Technological advancements in mobile computing and changes in working practice have heralded an age which encourages access to information at any time and at any place. Whilst the new-found flexibility is welcomed by many employees and internet users, there are many more risks to be addressed in terms of ensuring secure access to the corporate ICT systems, especially with the proliferation of tablet devices and smart mobile phones. Employees, guests and students seek access to corporate and business information on personally owned devices rather than using the corporately owned computing infrastructure.

The purpose of the procedure is to provide guidance to College staff and students on acceptable use of portable media and to provide guidance on accessing College network and systems from remote locations

15.2 Definition of Mobile Computing

There are two ways to access corporate data when working is a remote location. These are:

- Remote Access – The process of accessing information in a web browser or via a 'remote desktop' solution over the internet. The information remains at source and is never copied to the local device.
- Offline Remote Access – This is the process of copying data to a secondary storage device so that it can be accessed offline, i.e. without an internet connection.

Common categories of portable devices/media are listed below although this list is not exhaustive:

- Laptops, MacBooks
- Tablet computers
- Mobile phones with messaging capability and data storage
- USB memory sticks
- Other media such as DVDs, portable hard drives, MP3/MP4 players, camera memory cards

15.3 Working with portable media and devices

The following guidelines should be adhered to:

- Personal, sensitive or confidential information should not be stored on any portable device unless that device supports encryption and has been approved for use by a College authority in the role of Network Manager or above.
- Only encrypted devices should be used for storage of personal or confidential data.
- Persons using portable media must ensure that devices are not left unattended in public places.
- Portable devices must be adequately secured (e.g. laptops are not left logged on).
- Loss of portable devices must be immediately reported to the staff member's Unit Head or Head of School, or student's lecturer (in case of students). If it has been established that personal or confidential data has been stored on the stolen device,

the incident will be escalated to the Information & Cyber Security Committee (ICSC). (Please refer to section 12.0 ICT Security Controls and Incident Procedure).

- College owned laptops must be connected to the College network at least once per week for anti-malware, application and operating system updates.
- College owned laptops must have data encryption enabled on the local hard drive. (This is dependent upon hardware capability to support encryption method).
- College provided mobile phones with messaging capability must have a pin number or password set on the handset.

Bringing in Your Own Device (BYOD)

Non College-owned computing devices (laptops, tablets, MacBooks) can be used within the College as long as critical updates have been applied (e.g. Anti-malware, operating system and application). Connection to the eduroam wireless network is permitted. However, staff or students who chose to access the wireless network through their own devices do so at their own risk. The College will not be responsible for any damage, data loss or corruption during or after connection to the wireless network.

15.4 Data Control and Authority

As data controller, SERC must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing. Staff are required to store College information and data securely. This applies equally to information held on the College systems and to information held on an employee's own device.

Conditions

The College permits access to the following ICT services with personally owned or third party devices as long as:

- Internet/intranet access – the device, (PC, laptop, MacBook or tablet), has up-to-date anti-malware software, critical operating system and application updates installed. Access to the College network will be via the eduroam wireless network. Staff or students who chose to access the wireless network through their own devices do so at their own risk. The College will not be responsible for any damage, data loss or corruption during or after connection to the wireless network.
- No data classified as personal, sensitive or confidential is stored on them. Any information deemed personal, sensitive or confidential must be deleted or removed immediately. In the context of e-mail messages, the Deleted Items folder must also be emptied.
- Staff members must familiarise themselves with the device sufficiently in order to keep the data secure. In practice, this means:
    - preventing theft and loss of data,
    - where appropriate keeping information confidential and
    - maintaining the integrity of data and information.

Staff members should:

- Delete sensitive, confidential or commercial emails once finished with them.
- Delete copies of attachments to emails such as spread sheets and data sets on mobile devices once finished with them.
- Limit the number of emails and other information that are synced to their device.

Loss or Theft

In the event of a loss or theft, the password to all College systems accessed from the devices should be changed (and it is recommended this is done for any other services that have been accessed via that device, e.g. online banks, etc.).

Any loss or theft of a device should be reported promptly to the College IT & Services Department. It may be necessary to invoke a "remote wipe" of the device. It is recognised that remote wiping of data may result in the loss of the employee's personal information held on the device. A "remote wipe" will not be carried out without consultation with the device owner.

Security and Integrity of the Device

Staff are required to play their part in maintaining a safe working environment and in terms of BYOD, this means keeping software up to date and avoiding content that threatens the integrity and security of their device(s), the College systems and the devices of other staff or students. The College will enforce a security policy on each mobile phone that is granted access to e-mail. This will force the setting of a pin number/password. The phone will automatically lock after two minutes of inactivity.

Monitoring of User Owned devices

In exceptional circumstances, the College may require access to College data and information stored on your personal device. In those circumstances, every effort will be made to ensure that the College does not access the private information of the individual. College data and information can only be stored and processed on personally owned devices under acceptance of these conditions.

15.5 Remote Computing

"Remote Computing" for the purposes of this procedure, can be defined as accessing any College system from a device in a location that is not part of, or directly connected to the College data network. It includes accessing the College network from home or external workplaces.

Working from a remote location

The College will provide a secure connection for remote access such as TLS (Transport Layer Security), VPN (Virtual Private Network), or other secure method.

The following guidelines should be adhered to when working from a remote location in terms of accessing College ICT systems:

- Devices used from a remote location must have updated anti-malware software installed.
- Only College staff will be permitted to access College ICT systems from remote locations. Third parties are not permitted to access College systems from a College staff or student member's user account. It is incumbent upon staff and students to ensure that they do not disclose password details to any third party and that they ensure that they have logged off from the College system and remote device before leaving the same device.
- Any files to be copied to a College storage area must be malware checked in first instance by the person wishing to copy or upload the file. Infected files must not be copied.
- It is not permitted to copy large files from a remote location to a College server unless prior consent from the IT & Services department has been granted. File compression utilities should be used on any file over 50MB (megabytes) in size.

15.6 General Guidelines

Version Control

Due care must be taken when working remotely or with copies of source documents on portable media that appropriate version control takes place. By default, versioning is turning on in all Office 365 TeamSite's, Groups & OneDrive. This facility will maintain an unlimited number of version

Files hosted on existing file shares It is recommended that copy documents have a version number appended to the file name (e.g. mobilecomptingVer1.doc). Each document should also have a date of revision, author and name added to the document footer. The source document should only be overwritten with the approved version. Approval should be sought from Departmental Heads in situations where documents are to be copied to shared departmental drives.

Copy documents should be deleted once the approved document has been uploaded to the appropriate storage area.

Use of Third Party Devices

Users of third party devices requiring networking connectivity other than via the wireless network, must seek prior permission from the IT & Services Department.

Wireless networking

The College does provide comprehensive wireless access across all campuses. The eduroam wireless network service is available to staff and students to use on college-provided or on personally owned devices. Authentication is required via a valid staff/student e-mail address and password. Each laptop ought to have the latest anti-malware software definitions installed and should have the latest operating system (Windows/OSX) updates applied.

It is not permissible for anyone to connect any wireless access point to the College network or indeed to connect any device to the College wired network. ICT personnel only are permitted to carry out such tasks.

16.0 Communication Plan

This Procedure will be uploaded to the College intranet and referred to in staff induction and training.

17.0 Review

Procedures associated with ICT security will be reviewed at least every 12 months. Additional reviews and updates will take place inside that timeframe if new systems are implemented and/or if significant infrastructural changes take place (e.g. new campuses connected to the network, server installations and refurbishments).

Appendix 1: Document Change History

Date of Change	Approved By	Change Detail
13/03/2021	A Emmett	Added change history as appendix to track changes, resulting in renumbering of document.
18/04/2021	A Emmett	Section 3.4 – Added further clarification regarding default config Section 4.6 – Added clarification regarding process for requesting access to systems. Section 5.6 – Added information about tooling used to monitor activity/security of college systems Section 5.7 – Added reference to Microsoft Security Centre Network Isolation feature Section 9.5 – New section clarifying expectation in relation the update of network connected devices Section 9.8 – Updated guidance in relation to 3rd party access. Section 13.2 – Removed reference to Public classification of data following on from feedback from DPO

Appendix 2: ICT Systems Managers

System Name	
QLS	Head of Knowledge Management
Agresso	Financial Controller
Jane HR	Senior HR Business Partner Financial Controller
TfS	Chief Training and Contracts Officer
Syllabus Plus	Head of Knowledge Management
Web Services	Chief Technology Officer
Security Access System, Energy Management	Head of Estates and Facilities Management
E-mail, web, file, network access	Chief Technology Officer
Library Systems (Booking and Catalogue)	Head of Quality, Excellence and Development

Appendix 3: Incident Report Form

Form on next page

SERC
INSPIRING. TRANSFORMING. ENRICHING.

IT & Services

Information Security Incident Report

This form should be used to report Information Security incidents, such as:

- Suspected virus/worm/Trojan/ransomware infection
- ICT hardware or software theft, damage or loss
- Inappropriate use of College ICT facilities or services
- Loss of sensitive or valuable information, i.e. student records, exam papers, financial records
- Suspected breach of Information Security or ICT Policies.

Details of Person Reporting Incident	
Full Name:	
Contact Number:	
Email:	
School/Department:	

Details of Incident				
Date/Time of Incident:				
Is Incident still in progress?	Yes		No	
Do you need assistance from Information Security?	Yes		No	
Has this Incident already been reported to Service Desk?	Yes		No	
If Yes, provide Service Call number:				

Comments