

## **ICT Systems & Services SOP**

**SOP Number:**  
206-10-2015

**Academic Year:**  
2025/2026 Onwards

**Date Of This Issue:**  
May 2026

**Responsible Owner:**  
Chief Technology Officer

### **Summary of Contents**

ICT Services Procedures, including:

- Access Control
- Anti-malware & Anti-Spyware
- Email and Messaging
- Internet Use
- Network Management
- Password
- Security
- Vulnerability Management
- Software Licensing Management
- Data Management
- Remote Access & Mobile Computing
- Training & Awareness
- List of ICT Systems Managers

### **Review Information (Responsible Owner):**

First Created: 30 September 2015

Last Reviewed: May 2026

Next Review: April 2027

### **Change Type at last Review:**

No/Minor/Significant

### **Approval/Noting By:**

CMT: 7 May 2026

### **Previous Reference (for control purposes):**

155-05-2014: ICT Systems and Services  
SOP

189-06-2015: Social Media SOP

### **Date of Equality of Opportunity and Good Relations Screening (Section 75):**

October 2016

### **Date of Last Accessibility Screening:**

June 2025

<b>1.0</b>	<b>CHANGE HISTORY</b>	<b>3</b>
<b>2.0</b>	<b>ABBREVIATIONS</b>	<b>3</b>
<b>3.0</b>	<b>BACKGROUND</b>	<b>5</b>
<b>4.0</b>	<b>SCOPE</b>	<b>5</b>
<b>5.0</b>	<b>ACCESS CONTROL PROCEDURE</b>	<b>6</b>
5.1	INTRODUCTION	6
5.2	ACCESS CONTROL RULES	6
5.3	ALL USERS	6
5.4	ACCESS CONTROL RULES – SYSTEM AND NETWORK ADMINISTRATORS	6
5.5	TYPES OF ACCESS CONTROL EMPLOYED	7
5.6	MONITORING AND REVIEW OF ACCESS	7
5.7	REPORTING OF INCIDENTS	7
5.8	REQUESTING ACCESS	7
<b>6.0</b>	<b>SECURITY &amp; ENDPOINT PROTECTION PROCEDURE</b>	<b>8</b>
6.1	INTRODUCTION	8
6.2	DEFINITIONS OF MAIN MALWARE TYPES	8
6.3	SUSCEPTIBILITY	8
6.4	PREVENTATIVE MEASURES	8
6.5	LEVELS OF PROTECTION	10
6.6	MONITORING & REPORTING	10
6.7	DEALING WITH A MALWARE INCIDENT	11
6.8	DELIBERATE MALWARE INTRODUCTION	12
6.9	LIABILITY	12
6.10	END USER SECURITY TRAINING & TESTING	12
6.11	ADDITIONAL SECURITY RECOMMENDATIONS (PERSONAL DEVICES)	12
<b>7.0</b>	<b>ELECTRONIC FILE SERVICES PROCEDURE</b>	<b>13</b>
7.1	INTRODUCTION	13
7.2	ACCEPTABLE USE OF COLLEGE ELECTRONIC FILE SERVICES	13
7.3	GENERAL GUIDANCE	13
7.4	ONEDRIVE	13
7.5	SHAREPOINT/TEAMS	14
7.6	LEGACY FILE SHARES	14
7.7	PROTECTING ELECTRONIC FILE SERVICES	14
7.8	BREACH OF GUIDELINES	14
7.9	STAFF AND STUDENT LEAVERS	14
<b>8.0</b>	<b>EMAIL AND MESSAGING PROCEDURE</b>	<b>16</b>
8.1	INTRODUCTION	16
8.2	GENERAL GUIDANCE	16
8.3	EMAIL (EXCHANGE ONLINE)	16
8.4	MICROSOFT TEAMS	16
8.5	ACCEPTABLE USE OF EMAIL AND MESSAGING	16
8.6	DEALING WITH DUBIOUS OR SUSPICIOUS EMAILS	17
8.7	BREACH OF GUIDELINES	18
8.8	STAFF AND STUDENT LEAVERS	18
<b>9.0</b>	<b>INTERNET USE PROCEDURE</b>	<b>20</b>
9.1	INTRODUCTION	20
9.2	ACCEPTABLE INTERNET USAGE	20
9.3	UNACCEPTABLE INTERNET USAGE	20
9.4	ACCESSING AND USE OF SOCIAL MEDIA AND BLOGGING WEB SITES	21
9.5	REPORTING OF INCIDENTS AND MAKING A COMPLAINT	21
<b>10.0</b>	<b>NETWORK MANAGEMENT PROCEDURE</b>	<b>22</b>

10.1	INTRODUCTION .....	22
10.2	PURPOSE .....	22
10.3	DEFINITIONS .....	22
10.4	PROCEDURE .....	22
10.5	UPDATE OF SYSTEMS.....	23
10.6	NETWORK ACCESS .....	23
10.7	FAULT MANAGEMENT & END USER SUPPORT.....	24
10.8	REMOTE ACCESS.....	24
10.9	THIRD PARTIES.....	24
10.10	USER ACCOUNTS FOR STAFF AND STUDENTS .....	25
<b>11.0</b>	<b>PASSWORD PROCEDURE.....</b>	<b>27</b>
11.1	INTRODUCTION .....	27
11.2	PURPOSE .....	27
11.3	SCOPE .....	27
11.4	PROCEDURES FOR COLLEGE SYSTEMS.....	27
11.5	GENERAL PASSWORD GUIDELINES .....	27
11.6	PASSWORD PROTECTION STANDARDS .....	28
11.7	FEDERATED IDENTITY & SSO .....	29
11.8	ADDITIONAL SECURITY MEASURES (2FA/MFA).....	29
11.9	CHANGING/RESETTING PASSWORDS .....	30
11.10	PASSWORD MANAGERS .....	31
11.11	ENFORCEMENT.....	31
<b>12.0</b>	<b>VULNERABILITY MANAGEMENT .....</b>	<b>32</b>
12.1	INTRODUCTION .....	32
12.2	ROLES & RESPONSIBILITIES .....	32
12.3	IDENTIFICATION OF VULNERABILITIES .....	33
12.4	PRIORITIZING & MITIGATING VULNERABILITIES.....	34
12.5	LEGACY DEVICES & EXCEPTIONS .....	35
<b>13.0</b>	<b>ICT SECURITY CONTROLS AND INCIDENT PROCEDURE.....</b>	<b>37</b>
13.1	INTRODUCTION .....	37
13.2	REQUIREMENTS FOR SECURITY CONTROLS.....	37
13.3	SECURITY - GOOD PRACTICE GUIDELINES.....	38
13.4	PROCEDURE FOR REPORTING A SECURITY INCIDENT OR SECURITY VULNERABILITY .....	39
13.5	RESPONSIBILITIES FOR INFORMATION SECURITY.....	39
13.6	LINKS WITH OTHER BODIES .....	40
13.7	RESPONSIBILITY .....	40
13.8	FURTHER INFORMATION .....	40
<b>14.0</b>	<b>SOFTWARE LICENSING MANAGEMENT PROCEDURE .....</b>	<b>41</b>
14.1	INTRODUCTION .....	41
14.2	ACCESS .....	41
14.3	METHOD OF INSTALLATION .....	41
14.4	AUTHORISATION.....	41
14.5	CONTROL .....	42
14.6	PROCUREMENT AND RECORDING.....	42
<b>15.0</b>	<b>DATA MANAGEMENT PROCEDURE.....</b>	<b>43</b>
15.1	INTRODUCTION .....	43
15.2	CLASSIFICATION OF DATA TYPES.....	43
15.3	MANAGEMENT OF ELECTRONIC DATA – PROTECTED & RESTRICTED CLASSIFICATIONS .....	44
15.4	RETURN, DISPOSAL AND TRANSFER OF PHYSICAL MEDIA.....	47
15.5	SECURITY.....	48
15.6	ASSET AND INVENTORY MANAGEMENT .....	48
15.7	ACCESS TO DATA.....	48
15.8	DISCOVERY OF INAPPROPRIATE DATA, FILES, IMAGES.....	50
15.9	DISCLOSURE OF INFORMATION .....	50

15.10	GOOD PRACTICE GUIDE ON DATA MANAGEMENT AND ICT SECURITY.....	50
<b>16.0</b>	<b>REMOTE WORKING, BYOD &amp; 3<sup>RD</sup> PARTY ACCESS.....</b>	<b>54</b>
16.1	INTRODUCTION .....	54
16.2	MANAGED DEVICES.....	54
16.3	UNMANAGED DEVICES – BRING YOUR OWN DEVICE (BYOD) .....	55
16.4	GEOGRAPHICAL RESTRICTIONS WHEN TRAVELLING.....	57
16.5	REQUESTING TEMPORARY REMOVAL OF GEOGRAPHICAL RESTRICTIONS .....	57
16.6	GENERAL GUIDELINES .....	58
<b>17.0</b>	<b>TRAINING &amp; AWARENESS .....</b>	<b>58</b>
17.1	IT & SERVICES TRAINING CATALOGUE .....	58
17.2	ALLOCATION OF TRAINING & TIMESCALES FOR COMPLETION .....	59
17.3	SECURITY TESTING.....	59
17.4	MONITORING & ESCALATION ROUTES .....	60
<b>18.0</b>	<b>COMMUNICATION PLAN.....</b>	<b>61</b>
<b>19.0</b>	<b>REVIEW.....</b>	<b>61</b>
	<b>APPENDIX 1: DOCUMENT CHANGE HISTORY .....</b>	<b>62</b>
	<b>APPENDIX 2: ICT SYSTEMS MANAGERS .....</b>	<b>64</b>
	<b>APPENDIX 3: INCIDENT REPORT FORM.....</b>	<b>65</b>

## 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.

### ***BYOD (Bring You Own Desktop)***

A special configuration that allows personally owned devices to access college resources.

### ***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.

### ***Managed Devices***

Devices including smartphones, Computers/Laptops running Windows/macOS/ChromeOS and tablets running iOS & Android that are owned, configured & monitored by the College.

### ***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.

***Unmanaged Devices***

Devices including smartphones, Computers/Laptops running Windows/macOS/ChromeOS and tablets running iOS & Android that are owned by the end user.

***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) and all College owned computing devices (managed devices).

## **5.0 Access Control Procedure**

### **5.1 Introduction**

The business requirements for access controls on computer systems are:

- Protection of protected or restricted information from unauthorised access.
- Ensuring data integrity in terms of preventing deliberate or accidental modification or deletion.

### **5.2 Access Control Rules**

#### **5.3 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

#### **5.4 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, Cloud Service 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](#)).
- All administrative accounts must be secured with 2FA/MFA
- The ability to make configuration changes is restricted to Managed Devices. In addition, these devices must be hosted on a secure, on premise college subnet.

## **5.5 Types of Access Control Employed**

The type of access control that will be used include:

### **5.5.1 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.

### **5.5.2 File System Controls**

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

### **5.5.3 Computer System Controls**

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

### **5.5.4 Network Controls**

Protection of the College network will be achieved using firewalls, access control lists, 802.1x access 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 be those that are required to complete the function of the device.

### **5.5.5 Authentication Controls**

Schemes such as Username & Password, 2 Factor Authentication, FIDO, Windows Hello and 802.1x.

## **5.6 Monitoring and Review of Access**

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

## **5.7 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.

## **5.8 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 [15.7](#).

## **6.0 Security & Endpoint Protection 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 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/Keyloggers – is a computer program that records or captures information from an infected computer without the knowledge of the computer user.
- Rootkits – This type of malware gives hackers remote control of a victim's device.
- Exploits – This type of malware takes advantage of security vulnerabilities in applications or operating systems.

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 Endpoint Protection product that provides coverage for all servers and end user devices<sup>1</sup>, including anti-malware, behavioural monitoring, ransomware mitigation & centralised management & reporting. The product is configured to update on all servers and end user devices directly when latest updates are available from the vendor's update repository, normally every 8 hours. Non-protected & out of date devices are proactively identified using compliance monitoring policies provided by the product.

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

- Operating System critical software updates should be applied within 14 days of release, with the following constraints:
  - For end user devices, organisational rollout should start after a 1 day pilot with a smaller group of devices. When issues occur, they should be noted in the Security Operations Log.
  - For servers and other network equipment, 1 element of a cluster or HA solution should be piloted for 1 least one day. When issues occur. they should be noted in the Security Operations Log.
  - Where there is no resiliency for a specific solution, a rollback plan should be in place where possible.
- All Servers and end user devices 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 to disable or to attempt disabling of automatic update to the anti-malware software.
- All College-owned laptops and PCs must be connected to the College network or internet at least once per week to facilitate anti-malware updates.
- Personally owned laptops/PCs/Tablets and Mobile Phones must be kept updated, and where available, 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 such as 'Torrent' networks, due to the extremely high risk of virus introduction.
- Download, installation or use of spyware software on production networks is forbidden. If required, special supervised network will be configured for specialist courses such as Cyber Security.
- Unexpected or suspect e-mail messages with or without attachments must be reported using the 'Report Message' function in Outlook or 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.

<sup>1</sup> *Devices refers 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<sup>2</sup> 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.

## 6.6 Monitoring & Reporting

There are 3 key tools that are used by ITS to monitor the health of the network. These are:

### **Microsoft 365 Security Centre**

The Centre monitors & manages the antimalware software on all workstations, servers & mobile devices. It uses central reporting to automatically notify administrative staff about any malware, unwanted software & suspicious program/user behaviour on devices. This includes a forensic log of all device activity to allow for troubleshooting and to aid investigations in the event of a cyber event. It also maintains an inventory of all managed devices including the OS, installed applications and any vulnerabilities.

The Centre also 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.

The Centre also contains a recommendation engine that can be used to progressively improve the security profile of network and any associated cloud services. It uses a range of telemetry data from its inventory & configuration repository to generate a measure known as ‘Secure Score’. Secure score is an important part of SERC’s approach to ensuring the secure configuration of its network. The college has a target to keep its secure score above 80%.

### **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 Intune**

Microsoft Intune is a Mobile Device management solution used by the college to manage mobile phones, tablets as well as traditional PC/Mac platforms. The solution contains a wealth of hardware & software inventory data as well as the ability to assess security compliance, assign policy and even remotely erase the devices.

ITS staff proactively monitor the status of above solutions daily. 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 via the College ServiceDesk or at one of the local campuses: Bangor, Downpatrick, Newtownards or Lisburn.

## **6.7 Dealing with a Malware Incident**

Should an incident take place the following procedure will be followed:

- The incident should be reported immediately to the Chief Technology Officer (CTO) or in their absence, Head of Networks (HoN), outlining the nature & scope of the incident.
- CTO.HoN Officer to inform CMT, ICSC, Heads of School and Unit Heads of scope and scale of disruption.
- If required, the CTO/HoN will inform the Colleges Cyber Security Insurer.
- 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.
- A decision will be taken based on an assessment of the situation as to whether the compromised machine/s will be retained for further investigation, cleansed or re-imaged.
- 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 serious or major 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 malware 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 End User Security Training & Testing**

There is an ongoing threat to the College from cyber criminals who are continuously attempting to breach the security mechanisms put in place to protect college systems. These may take the form of phishing attacks, social engineering, password leakage via data breaches etc

The college is committed to the safety of all its users and college information. To address this threat, the College will ensure that training resources are made available to all system users in relation to data protection, online safety and phishing. The college will also reinforce this training by performing security testing at least twice a year for all staff, students & governors.

The results of this testing will be reported to the College ICSC.

## **6.11 Additional Security Recommendations (Personal Devices)**

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

- Ensure your device's Firewall is always turned on. 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 daily.
- Ensure that your device is set up 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 applications 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 vendor's site and not another source.

## **7.0 Electronic File Services Procedure**

### **7.1 Introduction**

All users at some point will require to save files into a storage repository. The College provides 2 preferred services for the store of files, both cloud based. These are OneDrive for Business & SharePoint Team Sites.

In some niche cases, there may be a requirement for a legacy File Share, mapped to a drive letter, hosted on a college server.

The college strongly discourages the use of removable storage devices (e.g. USB keys, removable hard drives) for the transportation of any data, but particularly for 'Protected' or 'Restricted' data. More guidance is available in [15.3](#) 'Data Management Procedure' section of this document.

### **7.2 Acceptable use of College Electronic File Services**

All storage provided by the college is intended for the purposes laid out in the college Acceptable Use Policy. In summary:

- For students, this includes research and assignment work.
- For staff, this includes administrative, teaching and research activities.

Occasional and moderate use of College File Service facilities for private use is permitted, provided users act in accordance with UK law, anything stored on these services does not negatively impact access for others, and does not contravene international laws or treaties.

Personal information stored on college systems is also the responsibility of the end user. The College do not take responsibility for the recovery of this information in the event of a disaster.

### **7.3 General Guidance**

By default, access to cloud services is limited to UK & Ireland based access. However, when travelling internationally on College Business or trips, users may request the temporary removal of their travel restrictions for a defined period. Requests should be made to the College IT department via the Service Desk App.

### **7.4 OneDrive**

OneDrive is a Cloud based file storage solution intended for users to hold file that are considered personal/private and are only accessible by the user who is associated with the OneDrive. This allows the user to benefit from scenarios such as working from home and the use of BYOD devices. The service also provides a range of other features such as Versioning, Recycle Bin, browser-based viewing/editing of files and sharing capabilities.

All Staff & Students will be provisioned with a OneDrive and will be allocated 25GB of storage for files by default, although the default storage quota can be raised upon request the College IT department.

When sharing a file or folder with one or more users, users are reminded that it is their responsibility to ensure that files are shared appropriately, and that the college is not liable for the loss or exposure of personal information that has been shared by the account holder.

## **7.5 SharePoint/Teams**

SharePoint Online is a collaboration tool that provides collaborative shared storage to groups of users. This storage service is also the backend for Microsoft Teams, meaning that information stored within Microsoft Teams will reside in an underlying SharePoint Team Site.

Team Sites & Microsoft Teams are most used when there is a requirement for more than 1 user to collaborate, co-edit and share files. The type of site can be either:

- Private – Accessible to only a pre-defined set of members.
- Public – Accessible to anyone within the organisation.

The most commonly used site type is a Private Site. Examples are Departmental File Storage, Projects and Class Collaboration areas for user in curriculum.

All Team Sites will be allocated 15TB of storage for files by default, although the default storage quota can be raised upon request to the College IT department.

If files stored in a Team Site will contain protected or restricted personal or commercial information, strong controls should be implemented in relation to the security and membership of the site. The College IT department can provide further guidance on request on a case-by-case basis.

## **7.6 Legacy file shares**

The College no longer uses legacy SMB/NFS file shares, outside of specific needs relating to the delivery of Core IT infrastructure services. If a requirement arises relating to delivery of end user services or relating to a specific application, this will be provided on a case-by-case basis, and only when other approaches have been exhausted.

## **7.7 Protecting Electronic File Services**

All on premise data will be backed up according to the guidance is available in '[15.3 Data Management Procedure](#)' section of this document and the College 'Backup & Restore' SOP. Data held in Cloud based storage has built-in protections against issues such as ransomware and accidental deletion.

## **7.8 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.

## **7.9 Staff and Student Leavers**

Access to files is governed by the Active/Expired/Disabled status on the associated user account. Refer to section 11.9 for more info on when these statuses are set.

When a staff member leaves the College, files in their OneDrive & Personal File Shares will be deleted 210 days after leaving date. At 180 days after their leaving date, their account will have its Office 365 license removed, at which point a grace period of 30 days will begin. When the end of this grace period has been reached, all email will be permanently deleted, with no option for recovery. Files held in Personal File Shares will be deleted at the 180-day deadline, with a temporary option to retrieve this data from the college backup system for 30 days.

Final year students will have their OneDrive deleted 210 days after the end of the academic year, normally 30<sup>th</sup> June. This rule also applies to students who have withdrawn early, or who have been excluded, although their access may have been revoked early by disabling their account. At 180 days after the end of the academic year, their account will have its Office 365 license removed and the account will be disabled. At this point a grace period of 30 days will begin. When the end of this this grace period has been reached, all files will be permanently deleted, with no option for recovery.

It is the responsibility of users & their line managers/lecturers to ensure that any business-critical or assessment materials have been filed in a shared repository before they leave employment/study.

In exceptional circumstances, with the approval of the Chief Executive, a staff/governor leaver may retain access to their email account, for a defined period, following their date of leaving. All other licencing, distribution group membership, services & permissions will be removed.

## **8.0 Email and Messaging Procedure**

### **8.1 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.

### **8.2 General Guidance**

By default, access to cloud services is limited UK & Ireland based access. However, when travelling internationally on College Business or trips, users may request the temporary removal of their travel restrictions for a defined period. Requests should be made to the College IT department via the Service Desk App.

### **8.3 Email (Exchange Online)**

Exchange Online is a Cloud based email & productivity solution provided to users to allow communication via email, calendaring, contact management & task management tools.

All Staff & students will be provisioned with a Mailbox and will be allocated 25GB of storage for content by default, although the default storage quota can be raised upon request the College IT department.

In addition to personal, 'Shared Mailboxes' can provide to department where collaborative features are needed, such as departmental email address that is monitored by a team and can be used to send emails from a departmental identity instead of an individual.

### **8.4 Microsoft Teams**

Microsoft Teams is a collaborative hub for teamwork that enables instant messaging, audio and video calling, rich online meetings, mobile experiences, and extensive web conferencing capabilities. It is used heavily with the college, especially in scenarios such as distance learning and the facilitation of Online meetings/training.

All Staff & Students will be allocated with a Microsoft Teams licence.

### **8.5 Acceptable use of Email and Messaging**

The following guidelines must be adhered to:

1. 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.
2. Email should be used for SERC business; teaching or study-related activities provided such activities are legal.
3. Use for personal activities such as shopping, banking etc is strongly discouraged and all users should work towards the separation of personal email into another service provider such as outlook.com or Gmail. Assistance can be sought from the college IT department if required.
4. 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.

5. In order to reduce the risk of malware infection, users should not open file attachments of any file type unless:
  - a. It is a Microsoft Office file (i.e. Word document, Excel spreadsheet) or PDF and
  - b. It is a file that they are expecting to receive or has been sent to them from a known and reputable source.

*Please report dubious mail messages or check with ITS Department for advice (see Section [8.6](#) for more information).*

6. Users must not e-mail or message any illegal, malicious or copyright protected files or information.
7. Users are not permitted to use the College email and messaging services as a medium to transmit offensive or abusive material or messages.
8. 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.
9. 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 protected or restricted information should be reported and deleted.
10. Each user is responsible for managing the content of their mailbox. There is an expectation that each user will delete or retain processed messages from Mailbox folders in line with the college Retention & Disposal Policy. SERC cannot guarantee the integrity and indefinite storage of mailbox information.
11. 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.
12. All messages should be constructed observing acceptable etiquette. (For example, capital letters and large fonts should be avoided.)

## **8.6 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 any content that slips through using MS Outlook ‘**Report Message**’ facility. Note that reporting a suspicious email will also delete the email from the user mailbox.

## 8.7 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.

## 8.8 Staff and Student Leavers

Access to email is governed by the Active/Expired/Disabled status on the associated user account.

When a staff member leaves the College, their mailboxes will be deleted 210 days after leaving date. At 180 days after their leaving date, their account will have its Office 365 license removed, at which point a grace period of 30 days will begin. When the end of this grace period has been reached, all email will be permanently deleted, with no option for recovery.

Final year students will have their mailboxes deleted 210 days after the end of the academic year, normally 30<sup>th</sup> June. This rule also applies to students who have withdrawn early, or who have been excluded, although their access may have been revoked early by disabling their account. At 180 days after the end of the academic year, their account will have its Office 365 license removed, at which point a grace period of 30 days will begin. When the end of this this grace period has been reached, all email will be permanently deleted, with no option for recovery.

It is the responsibility of users & their line managers/lecturers to ensure that any business-critical or assessment materials have been forwarded or filed in a shared repository before they leave employment/study.

In exceptional circumstances, with the approval of the Chief Executive, a staff/governor leaver may retain access to their email account, for a defined period, following their date of leaving. All other licencing, distribution group membership, services & permissions will be removed.

## **9.0 Internet Use Procedure**

### **9.1 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 accesses 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.

### **9.2 Acceptable Internet Usage**

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

### **9.3 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.

#### **9.4 Accessing and use of Social Media and Blogging Web Sites**

The College will allow access to social media sites for staff and students as a general rule. If restrictions are required, teaching staff are expected to implement these with the provided classroom management software. If any concerns remain, they should be raised with the Head of Networks or Chief Technology Officer who will use their discretion in relation to the solution required to address the issue.

#### **9.5 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.

## 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:

- **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).
- **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 3<sup>rd</sup> party hosted Software as a Service (SaaS), Platform as a Service (PaaS) & Infrastructure as a Service (IaaS) functions.
- **Managed Devices** – College Owned PCs, Macs, Laptops, MacBooks, Servers, Workstations, or other devices that are not performing the function of a Network Component.
- **Managed Networks** – Network segments/VLANs that are reserved exclusively for college owned devices i.e. Managed Devices
- **Unmanaged Networks** – Network segments that are reserved for unmanaged devices such as BYOD devices.
- **Quarantine Network** – This is a default network segment with no access to other network segments & no access to the internet.
- **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.
- **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 within 2 weeks 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/application from the network.
- The College's cloud-based threat management tools provide an inventory of software and vulnerabilities.

## 10.6 Network Access

Access to the College network infrastructure is controlled by 802.1x authentication by both the Ethernet switching & Wi-Fi infrastructure. Access to network resources may be granted to either device or user context using the following guidance:

### 10.6.1 Wired Ethernet Access

Wired Ethernet networks shall be configured to ensure that only managed devices may connect to managed network segments.

User authentication to managed network segments should be blocked unless the device is a managed device.

Authentication configurations should be deployed using network policy such as Group Policy or MDM Configuration Profiles.

Unmanaged devices must be placed into a quarantine network and access to the internet or other network segments blocked when a wired ethernet connection is made.

### **10.6.2 Wi-Fi Access**

Wi-Fi access to managed network segments should be accessible to only managed devices.

Authentication configurations should be deployed using network policy such as Group Policy or MDM Configuration Profiles.

Wi-Fi access to unmanaged network segments must use the 'eduroam' service and authentication should be performed using a Staff or Student end user email address & password.

The college may, on an infrequent basis, allow 'Guest' access to unmanaged networks in addition to the provision of the eduroam service for the purpose of providing internet access to customers during special events such as Open days.

## **10.7 Fault Management & End User Support**

The IT & Services Department will operate a ServiceDesk 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 network team.

## **10.8 Remote Access**

For College staff only, VPN (Virtual Private Network) access to the College Network will be provided for managed devices only.

The College will provide remote access for staff and students as laid out in section [15](#).

## **10.9 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](mailto: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](mailto: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.

## **10.10 User Accounts for Staff and Students**

All Staff and students will be given a user account to log on to managed devices such as PCs/Macs/iPads when on campus and to access college services when working from home. This account is required to access e-mail, file storage, internet/intranet web-based services, eduroam Wi-Fi and other services.

Detailed procedures are outlined in the User Account Management SOP.

### **10.10.1 Staff**

The provisioning & management of user accounts for staff is enabled using data from the College HR system. In some cases, such as emergency appointments, the administration may lag behind immediate business needs. In this case, an email from the HR team will be considered sufficient evidence to proceed with the provisioning of an account.

Access to staff accounts will cease at the close of business on the day they leave, as recorded by the College HR system. An extension of 30 days may be authorised by the Head of Networks or the Chief technology Officer in order to complete administrative tasks. The access will be restricted to specific systems, normally the college PT Lecturer Claim App, HR Self Service Portal & Email. Access may be granted with the approval of the Head of Networks or the Chief technology Officer to other apps on a case-by-case basis.

In exceptional circumstances, with the approval of the Chief Executive, a staff/governor leaver may retain access to their account for an extended but defined period beyond 30 days following their date of leaving.

The situation may also arise where a staff leaver may wish to retrieve personal information from their account after leaving. The college will facilitate this situation, when possible, but the request must be approved by HR or the College Data Protection Officer. The requestor must only be allowed access under supervision to ensure that protected or restricted business information is not removed.

### **10.10.2 Students**

The provisioning & management of user accounts for students is enabled using data from the College Student Record system.

Final year students (those who are not expected to return in the next academic year) will have their account disabled 90 days after the end of the academic year, normally 30<sup>th</sup> June. This extended access is provided to allow continuity of study in the event that the student returns to study during the next academic year and to cater for course post completion tasks

such as remedial work or enrolling in the next academic year. If a student withdraws early or is excluded from their course, their account will be disabled as soon as the MIS system is updated. In the event of a suspension from their course, the account will remain active unless otherwise requested by the Course Coordinator, Deputy Head of School or Head of School.

## 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 15 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 this 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 Only Way 1s Up!
- H0ld the b1g 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](#).

Due to the use of 2FA for all user accounts, the college does not require that passwords are changed, so long as they meet complexity requirements. However, the college network team may enforce a password change if a specific concern arises. Password expiration is considered an outdated and ineffective practice when using stronger authentication methods such as 2FA. SERC procedures are based guidance from both NCSC & Microsoft.

Staff & students should not share SERC passwords with anyone, including classmates, administrative assistants or line managers. All passwords are to be treated as restricted. 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 3<sup>rd</sup> party websites are integrated with the colleges Identity Provider (IdP) in a configuration known 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 not permissible to have SSO enabled on a device that does not have a lockout time less than 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 be 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.
- In 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 Password Managers**

A ‘Password Manager’, sometimes also referred to as ‘Password Vault’, stores sensitive information in an encrypted form on a device such as a mobile phone. Access to the password repository is normally protected by a strong form of identity verification such as Fingerprint, Iris or Facial Scan.

The College considers password managers to be a useful tool and recommends the use of Microsoft Authenticator, which is a requirement for using SERC account 2FA and will therefore already be installed on a device. However, other password managers such as those provided by Google in the Android OS and by Apple in iOS/macOS are also considered suitable.

### **11.11 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 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 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 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 to appropriate disciplinary action.

## **12.0 Vulnerability Management**

### **12.1 Introduction**

In today's digital age, vulnerability management has become an essential aspect of maintaining robust cybersecurity within a business. Vulnerability management involves identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.

Effective vulnerability management ensures that the integrity, confidentiality, and availability of business-critical information and systems are maintained, which is crucial for operational continuity and compliance with regulatory requirements.

For this procedure, vulnerabilities are:

- Weak or no existent physical security
- Misconfiguration of Software/Hardware
- Flaws in firmware, operation systems or Applications

### **12.2 Roles & Responsibilities**

The college has two teams tasked with managing all computing devices and services. These teams are also responsible for addressing vulnerabilities on these devices and services. Their responsibilities are:

- Cloud & Server Infrastructure - Network Management Team
- End User Devices - Desktop Services Team

The responsibility for the identification, allocation of remediation tasks and monitoring of progress is performed by operational Cyber Security & Vulnerability group. The group consists of:

- Head of Networks
- Head of Desktop Services
- Network Manager (Cyber Lead)
- Chief Technology Officer

This group meets on a weekly basis and will:

- Review the results of penetration tests & vulnerability scans
- Identify & triage vulnerabilities
- Set remediation activity
- Monitor remediation activities
- Review training exercise when relevant
- Discuss Cyber issues affecting the education sector.

## 12.3 Identification of Vulnerabilities

As part of the IT technology stack, vulnerabilities normally exist due to human error in terms of unauthorised physical access, misconfiguration of a system or software flaw in firmware, hardware or applications.

The Cyber Security & Vulnerability group will monitor these areas of risk on an ongoing basis and will monitor, triage and address issues when they arise.

### 12.3.1 Physical vulnerabilities

Any sensitive computer or network devices must be kept in a restricted pass-swipe or physically locked location. Access to these areas must be restricted to authorised staff only.

Access control lists should be reviewed annually, documented and reported to the operational Cyber Security & Vulnerability group.

### 12.3.2 Misconfiguration Vulnerabilities

Where available, a configuration policy should be used to enforce settings for a device or software. This ensures configuration standardisation and allows for the centralised tracking and adherence to the configuration.

To identify misconfiguration vulnerabilities in hardware and software, the following tools should be employed:

- Penetration Tests (Annually)
- Network scans using Nessus (at least quarterly)
- Microsoft Secure Score (weekly)
- Microsoft Defender Vulnerability Management dashboard (weekly)
- Deviations from Policy based Configuration (weekly)
- Audits and reviews of configuration settings (annually)

Documentation relating to results of scans and remediation actions should be held on the IT & Services TeamSite and noted in the ICT Security Operations Log.

### 12.3.3 Software Vulnerabilities

Software vulnerabilities fall into 3 distinct categories.

#### **Firmware**

Firmware is software that sits at the hardware level for a device, normally embedded directly into the device's memory and is usually designed to control low-level operations. Hardware vendors release Firmware updates when a vulnerability is discovered.

## Operating System (OS)

This is the core software that manages a device's hardware and provides a platform for other software (applications) to run. In some scenarios, the terms of OS & Firmware may be used interchangeably. OS vendors release Firmware updates when a vulnerability is discovered.

## Application

This is software designed to perform a specific task, normally for a user, although in server scenarios, this may affect multiple users. Applications normally require an operating system to run. Application vendors release Firmware updates when a vulnerability is discovered.

All software vulnerabilities will be monitored using the following tools:

- Penetration Tests (Annually)
- Network scans using Nessus (at least quarterly)
- Microsoft Defender Vulnerability Management dashboard (weekly)
- Automated alerting or Intelligence feeds from vendors (ad hoc)

Documentation relating to results of scans and remediation actions should be held on the IT & Services TeamSite and noted in the ICT Security Operations Log.

### **12.3.4 Ad Hoc reporting**

In addition to structured centralised monitoring, vulnerabilities of any category may be reported by employees, students, contractors or members of the public. It is the responsibility of anyone in receipt of such information to relay this information to a member of the IT & Services team, which in turn should be relayed to a member of the operational Cyber Security & Vulnerability group for review.

Where possible, asset criticality ratings from MDE & Nessus scans should be used to guide prioritization.

### **12.4 Prioritizing & Mitigating Vulnerabilities**

In general terms, vulnerabilities with a CVSS v3 base score of 7.0 or above should be addressed within 14 days of discovery. However, there are other factors that may impact the prioritisation. These are details below:

#### 1. Internet-Facing Systems and Critical Assets

**Why:** Publicly accessible systems (e.g., web servers, email gateways, VPNs) are prime targets for attackers. Critical assets (e.g., databases with sensitive data) amplify risk if compromised.

**Action:** Prioritize vulnerabilities on these systems, especially those with high CVSS scores or exploitability. Ensure firewalls, routers, and servers are patched promptly (within 14 days).

#### 2. Critical and High-Risk Vulnerabilities (CVSS $\geq$ 7.0)

**Why:** These pose the highest risk of exploitation, potentially leading to significant data breaches or system compromise.

**Action:** Apply patches within 14 days of release, as mandated by Cyber Essentials. Focus on vulnerabilities with known exploits in the wild (e.g., listed in CISA's Known Exploited Vulnerabilities Catalogue).

**Examples:** Remote code execution (RCE) flaws, privilege escalation vulnerabilities, or unpatched software with active exploits.

### 3. Unsupported or End-of-Life Software

- a. **Why:** Software no longer receiving patches (e.g., Windows Server 2012, Adobe Flash) is highly vulnerable, as new exploits won't be mitigated.
- b. **Action:** Remove, replace, or isolate unsupported software in a segregated network with no internet access, per Cyber Essentials requirements.
- c. **Timeline:** Address immediately or as part of a planned upgrade cycle.

### 4. Medium-Risk Vulnerabilities (CVSS 4.0–6.9)

- a. **Why:** These pose moderate risk but may still be exploited, especially in combination with other vulnerabilities.
- b. **Action:** Schedule remediation after critical/high-risk issues, ideally within 30–60 days, depending on exploit likelihood and system exposure.
- c. **Additional Guidance:** Prioritize those with higher exploitability scores or affecting widely used software.

### 5. Internal Systems with Lower Exploitability

- a. **Why:** Vulnerabilities on internal systems with restricted access (e.g., behind firewalls) are less urgent but still require attention to prevent lateral movement by attackers.
- b. **Action:** Address these after external-facing and critical systems, within a reasonable timeframe (e.g., 60–90 days).
- c. **Tip:** Focus on vulnerabilities in software with a history of exploitation (e.g., Microsoft Office, Java).

### 6. Low-Risk Vulnerabilities (CVSS < 4.0)

- a. **Why:** These have minimal impact or exploitability but should not be ignored, as they could be chained with other vulnerabilities.
- b. **Action:** Plan remediation during routine maintenance cycles or bundle with other updates to optimize resources.
- c. **Timeline:** Typically within 90–180 days, depending on resource availability.

## 12.5 Legacy Devices & Exceptions

Sometimes, installing the latest version of the affected software might not fix the reported vulnerability, or there may not even be an update to address the issue. There are also cases where it might be appropriate not to update: for example, if the system is being decommissioned shortly and the vulnerability is hard to reach and hard to exploit e.g. in a secure or air gapped network segment.

The situation may also arise when the college may be unable to fix the issue because of constraints such as staff time, or concerns with compatibility of the updated software.

In these scenarios, the Cyber Security & Vulnerability group should risk assess the situation and ensure sufficient mitigations are in place to minimise the risk. General guidance is:

- Software that is no longer supported (end-of-life) must be removed from devices or isolated in a segregated network subnet with no internet access to remain compliant with Cyber Essentials.
- These systems should be placed under continuous monitoring until the software can be patched or decommissioned.

## **13.0 ICT Security Controls and Incident Procedure**

### **13.1 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.

### **13.2 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, [15.0](#) Data Management Procedure)
- Backup (See also [15.0](#) 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 are 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.

## **13.3 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 on all services when available.

## **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.

### **13.4 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.

### **13.5 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).

### **13.6 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

### **13.7 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.

### **13.8 Further Information**

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

## **14.0 Software Licensing Management Procedure**

### **14.1 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.

### **14.2 Access**

In order to prevent installation of unlicensed software, only IT & Services staff have the necessary access to install software that is not owned by the College and where licencing restrictions exist.

Access to install software is granted to the following personnel:

- Classroom/Office Managed Devices – IT & Services Staff only.
- Personally Assigned Managed Devices
  - All IT & Services Staff
  - All users, when using approved Self Service scenarios.
- Servers – Senior IT & Services staff only.

Scenarios outside those listed may occur, such as departmental Technicians or Software Development tasks. Requests should be made to the CTO/HoN will evaluate the requirement including scope & duration before approving the access.

### **14.3 Method of Installation**

There are three main methods available software installation:

- Central Deployment – Only IT & Services staff are permitted to deploy or authorise deployment of packaged software.
- Self Service Installation – A list of approved applications may be installed by a user on a managed, personally assigned device without administrative rights. This is done using the 'Company Portal' app which is preinstalled on the device.
- 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)

### **14.4 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.

## **14.5 Control**

All staff and students (other than scenarios stated above in Section [14.2](#)) 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.

## **14.6 Procurement and Recording**

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

## 15.0 Data Management Procedure

### 15.1 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.

### 15.2 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
- Protected
- Restricted

#### *‘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 ‘Protected’ & ‘Restricted’ categories.

#### *‘Protected’ 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.

***'Restricted' 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.

### **15.3 Management of Electronic Data – Protected & Restricted classifications**

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

#### **Storage and Transmission of Data**

- 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, Protected or Restricted 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, protected and restricted 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 Protected or Restricted 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. Protected or Restricted 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 Protected or Restricted 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, Microsoft Sensitivity may be used to securely transmit data.
- It is not permissible to store data classified as Protected or Restricted 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 the College Retention & Disposal Policy in line with statutory obligations.
- 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 beyond the required retention period.

- The College will not be responsible for loss of non-business data stored in its systems. Staff members or students should ensure that non business information & communication is held in repository not operated by 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 they 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. 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 passes the ‘Conditional Access’ requirement for the user requesting access.
- The device used is secured with the latest anti-malware software, that virus definitions are continually kept updated and a firewall is active on the device.
- 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”.

## 15.4 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 its 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 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:

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

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

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

## 15.5 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 the 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 [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](#) for further details on malware control)

## 15.6 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 [15.4](#) (Return, Disposal and Transfer of Physical Media).

## 15.7 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 either the Chief Technology Officer or a staff member in a Network Manager role.
- 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 or Head of Networks 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 or Head of Networks.
  - 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.
- A file or folder has been shared by the owner with another user using the Office 365 OneDrive 'Share' feature.
- 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.

### **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.

## **15.8 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.

## **15.9 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 3<sup>rd</sup> 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 3<sup>rd</sup> party, e.g Laptops or Servers during a Police investigation, a record of the asset must be 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 3<sup>rd</sup> parties.

## **15.10 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 (unless using 2FA)**
- **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/protected/restricted information on secure College storage systems i.e. Office 365 Teams/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/protected/restricted 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/protected/restricted information on a third party storage service 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 security in this scenario.
- 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.

## **16.0 Remote Working, BYOD & 3<sup>rd</sup> Party Access**

### **16.1 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 this new-found flexibility is welcomed by many 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.

Traditionally, access was restricted to College owned devices within College buildings. This requirement was necessary to protect sensitive College information and is still used.

However, the college also operates a framework under which all employees, guests, students & contractors who seek access to corporate and business information can do so on personally owned device. This framework is secure and supported by the college.

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, and to provide guidance on using personal devices.

'Remote Working' for the purposes of this procedure, can be defined as accessing any College on-premises or cloud hosted 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, other external workplaces or abroad.

### **16.2 Managed Devices**

College owned devices are referred to as 'Managed Devices'. Managed devices are configured and secured by the College. These devices include Computers/Laptops running Windows/macOS/ChromeOS and Phones/tablets running iOS & Android. These devices are fully managed with policy from Active Directory and the College MDM Solution These devices are deemed to have a higher security state and are actively monitored by the college anti-malware solution.

These devices are issued to facilitate college business and operate under the following baseline security configuration:

- The device is enrolled in the colleges Mobile Device Management Platform (MDM)
- Users have no administrative rights.
- The device must report back to MDM at least once every 13 days.
- At least one authentication challenge is required to access the device. This may include password/Pin/Biometric or other FIDO compliant technology.
- Critical software updates applied withing 13 days of release.
- An anti-malware solution is present and up to date in the device.
- A firewall is enabled on the device.
- The storge on the device is encrypted.
- The device will securely lock after 11 failed login attempts.

## **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. Remote VPN connections to on premise networks are only available to staff via college owned, managed devices.

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

- Users must ensure that devices are not left unattended in public places.
- Users must ensure that devices are locked when not being used.
- Devices used from a remote location must be compliant in the College Device Management Solution. Non-Compliant devices will be disabled unless there are mitigating circumstances.
- Only College users are permitted to access College ICT systems from remote locations. Third parties/family members are not permitted to access College systems from a College staff or student member's device or user account.
- Loss of managed 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 [13.0](#) ICT Security Controls and Incident Procedure).
- If you are planning to work i.e., are not on annual leave and are not within driving distance of the college, you should ensure that you have had approval from your Head of Department to work in this scenario as any IT failures e.g. a broken laptop will leave you unable to fulfil your contractual obligations.

### **16.3 Unmanaged Devices – Bring Your Own Device (BYOD)**

Normally owned by the end user, these devices include smartphones, Computers/Laptops running Windows/macOS/ChromeOS and tablets running iOS & Android. Unmanaged devices are always treated as 'Remote Devices', even when on College networks such as Eduroam in College buildings.

These devices can be used for college business when correctly configured, however, the following criteria must be met:

- The device is enrolled in the college's Mobile Device Management Platform (MDM)
- The device must report back to MDM at least once every 13 days.
- A 6-digit pin is set on the device
- Critical software updates applied within 13 days of release.
- An anti-malware solution is present and up to date in the device.
- A firewall is enabled on the device.
- The storage on the device is encrypted.

**Note - Windows/macOS/ChromeOS devices are not currently supported for BYOD**

Enrolment is performed by installing a small app known as 'Company Portal' on the user's personal device. When the user then launches the app, they will be asked to enrol their device in the college MDM solution. When enrolment has completed successfully, the device is classified as a 'Personal' device and managed separately from other college owned equipment.

Enrolling a personal device via MDM will enforce the required security levels and provide high level security information back to the college every 8 hours. This ensures that BYOD devices continue to meet the required security standards. This is known as the device being 'Compliant'.

It is important for users to understand that no personal information such as SMS, WhatsApp, photos etc from the device will be reported back to or be accessible to college IT staff. Data from College systems is held separately from their personal data on the device and the College will retain oversight over this data only. It is also important to note that if College IT staff have any security concerns relating to the device, the college reserves the right to remotely remove College data from the device without prior notice.

If a device fails to report back to MDM within 13 days, firewalls or antimalware protection has been disabled, or if security updates have not been applied by the 13th day of their release, the device will be deemed 'Non-Compliant'. Devices deemed as non-compliant will lose access to College IT systems until the device is brought back into compliance. The company portal app and system generated emails will normally advise the user in advance of the device becoming non-compliant & the app will suggest the required action to bring a device back into compliance.

When on campus, internet connectivity is enabled via the eduroam wireless network. Unmanaged devices will be limited to this network segment and are not allowed access to core managed networks.

Staff or students who choose to access the eduroam 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.

When using your own device, you must:

- Ensure that separate accounts are used on devices shared with family members.
- Ensure that pin codes and biometric security measures are not shared with others.
- Keep your device up to date with the latest security patches from your Hardware/Operating system/Anti-malware vendors.
- Ensure that security features provided by the manufacturer are not disabled or bypassed i.e. the device should not be 'JailBroken'
- Take care when connecting to insecure/unknown networks.
- Ensure you keep College information and data secure.
- Follow instruction from college IT staff, when necessary, in relation to College data.
- Agree to audits when required.
- Report any security/information security concerns or incidents to college IT staff.

- Report your device as lost so that the College can perform a precautionary 'Wipe' of College data from the device and remove it from its management system.
- Ensure that you 'factory reset' or 'fresh start' the device if you are disposing of the device or transferring ownership to another person. This protects both your own personal data and data belonging to the College. You should also notify College IT staff of the discontinuation of the device.

More information & guidance on BYOD is available from the IT Support Portal [www.serc.ac.uk/helpme](http://www.serc.ac.uk/helpme).

## 16.4 Geographical Restrictions When Travelling

To reduce the risk of unauthorised access to college systems, access to IT facilities is restricted by default to the UK & Ireland. When traveling outside this region, various restrictions are in place depending on where a user may attempt to access services from, as well as the type of devices being used. The following rules apply to all managed devices, user accounts on unmanaged devices & all college operated mobile phone voice & data contracts:

### **Travel within the UK/Ireland**

When traveling within the UK/Ireland, IT services will continue to work as normal. There is no need to notify College IT in relation to this sort of travel unless the user is a College mobile phone user. If the travel destination is the Republic of Ireland, the user will need to inform College IT so that international roaming can be enabled on the device's telephony service.

### **Travel within the EU**

When traveling to one of the 27 EU countries, the user will need to inform College IT of their intention to travel including the location they are travelling to, as well as the date of departure and date of return. IT will note this and temporarily allow travel for the duration of the trip, as well as enabling voice & data roaming on any College issued mobile phone if required.

### **Travel outside the EU (rest of world)**

As with travel within the EU, College IT will require advanced notice of a user's travel arrangements including location, date of departure and date of return. Access will be enabled for computing devices as with EU travel, however access to telephony voice and data services will be enabled only on a case-by-case basis. This is due to the high calling and data costs incurred with travel outside the EU.

## 16.5 Requesting Temporary Removal of Geographical Restrictions

Requests for temporary removal of geographical restrictions for international travel should be made at least 48 hours in advance of the date of departure via the College ServiceDesk (<https://servicedesk.serc.ac.uk>). The necessary option can be found under the category of 'International Travel Access' or by clicking this link [Create an International Travel Request](#).

In relation to any travel arrangements, users should remember:

- If you are on Annual Leave within the UK/Ireland, any access you are likely to require to stay in touch with the office will work as expected and you don't need to inform IT.
- If you are on a college trip with one or more cohorts of students, you should ensure you have informed IT about the students as well as yourself.
- All users (staff and students) travelling abroad will have MFA enforced on their devices when trying to access college resources.
- If you are on college trip with students and no other staff on the trip have access to a college mobile phone, we have in place a facility to borrow a phone for the duration of the trip.

## 16.6 General Guidelines

### Document 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 turned on in all Office 365 TeamSite's, Groups & OneDrive. This facility will maintain an unlimited number of versions and users are advised not to disable this facility.

### 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 personally owned devices. Authentication is required via a valid staff/student e-mail address and password. Each laptop should have the latest anti-malware software definitions installed and should have the latest available operating system (Windows/OSX/iOS & Android) security 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. Only ICT personnel are permitted to carry out such tasks.

## 17.0 Training & Awareness

The college offers a wide range of training and development to staff & students. The IT & Services Department is tasked with the development of training to end users relating to their personal safety and the safety of college systems & information. This training should be made available to staff via the Colleges Learning Engine platform and to students using the SERC4U Microsoft Teams app.

### 17.1 IT & Services Training Catalogue

The following training modules are maintained by the IT & Services Department:

- **Digital Safety** - This module advises staff & student on best practice in relation to protecting identity, devices, understanding phishing and other online risks. information.
- **Protecting Digital Data and Information** – This module advises on best practice when handling the different types of data within the organisation.

- **Access to Information and Document Disposal** – This module provides a working knowledge in the principles of information governance, requests for college related business information and how to dispose of records appropriately.
- **General Data Protection Regulations (GDPR)** – This module advises staff on the legislative requirements relating to UK & EU Data protection law.
- **Accessibility** – This module advises staff on the legislative requirements of the Accessibility Regulations 2018 and their responsibilities within the college.

Additional training & support material is also available on demand via the colleges IT Support Hub at <https://www.serc.ac.uk/helpme>. The Hub is maintained by the College IT Support team.

## 17.2 Allocation of Training & Timescales for Completion

All training is allocated as follows:

Module Name	Required at Induction/Enrolment	Undertaken every...
Digital Safety	All Users	12 Months
Protecting Digital Data & Information	Staff Only	24 Months (Staff Only)
Access to Information & Document Disposal	Staff Only	24 Months (Staff Only)
General Data Protection Regulations (GDPR)	Staff Only	24 Months (Staff Only)
Accessibility	Staff Only	24 Months (Staff Only)

All training modules should be completed within 30 days of being assigned to a user.

## 17.3 Security Testing

In addition to online training, the college should perform phishing exercises at least 3 times a year for all staff & students. In addition, targeted testing should be performed on smaller, more highly valuable groups throughout the year. These test, often refer to as 'spear phishing' and 'whaling', should be purposely customised to the target group or individuals to simulate a potential real-world threat. Groups for consideration when planning are:

- CMT
- Customer Services
- Finance
- Governors

- HR
- IT
- MIS
- Payroll
- Training Organisation

Testing should be performed using the Microsoft Defender Attack Simulation Training tool. This tool initiates, tracks and maintains records for all phishing exercises.

## **17.4 Monitoring & Escalation Routes**

### **General Training**

All training activity placed on Learning Engine is tracked automatically. When training is incomplete, staff and their line managers are emailed a summary of outstanding tasks on a weekly basis, giving line managers oversight and the ability to address incomplete training.

Incomplete training that has not been addressed by a line manager will be reviewed by the College Human Resources department during Integrated Monthly Performance Management Sessions (IMPMS). This is a standard monitoring function within the organisation which run every month and are used to hold budget holders to account and to raise performance issues with a department.

The Human Resources department will monitor any instances of incomplete training, and, unless there are valid mitigating circumstances, may initiate disciplinary action.

### **Security Testing**

All security testing training records will be kept centrally and tracked in Microsoft Defender Attack Simulation Training. High level record of tests & results must also be kept in the ICT Security Operations Log. The Cyber Security & Vulnerability group will monitor the results of all security exercises, such as Phishing tests.

Repeat offenders will be tracked and when a threshold of 3 sequential failures of a security test occurs, a meeting should be arranged by a member of the Cyber Security & Vulnerability group to understand and address the root cause of the failure.

The above process is intended to be supportive of the staff member. The college wishes to promote an environment of openness and honesty, as threats of disciplinary action can lead to a culture of misreporting or hiding of issues.

However, if there are further failures or the actions of the individual are deemed to be malicious, the Chief Technology Officer may make a referral to HR on competency grounds, and the individual may be subject to disciplinary procedures.

## **18.0 Communication Plan**

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

## **19.0 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 3 <sup>rd</sup> party access. Section 13.2 – Removed reference to Public classification of data following on from feedback from DPO
12/01/2023	A Emmett	Section 11.5 – Updated to reflect new password policy length requirement of 15 characters Section 11.6 - Removed reference to password expiration Section 11.10 - New Section providing guidance on use of password managers. Appendix 2 – Updated to reflect changes in Systems/roles.
02/02/2023	A Emmett	Section 7.x – Electronic File Services Procedure. This is a new section outlining how files are managed & retained/disposed. Section 9 – Removed Social Media Section & transferred to a standalone SOP owned by College Communications Department. Section 15.3 - Updated to provide new BYOD Guidance.
03/05/2023	A Emmett	Section 7.9 – Added paragraph to document conditions required for a leaver to retain access to their email.
07/11/2023	A Emmett	Section 13.3 - Updated section to indicate that Self Service Software installation available via 'Company Portal' app.
01/06/2023	A Emmett	Reviewed for accessibility.
17/10/2023	A Emmett	Section 7.4 & Section 8.3 - Revised default storage limits from 1TB to 25GB for OneDrive and 50GB > 25GB for Exchange Mailboxes to prepare for reduction in organisational storage allocation related to changes in Education Offering from Microsoft.
12/01/2024	A Emmett	Section 8.5 – Bullet point 3 added to encourage users to separate personal email use into a separate account. This will be come enforced at a future date. Section 14.2 - Sensitivity labels have been renamed. 'Confidential' now becomes 'Protected' & 'Sensitive' now becomes 'Restricted'
03/06/2024	A Emmett	Section 10.6 – Added new section detailing network access requirements. General – Fixed broken bookmarks General – Updated Job Titles following restructure

<b>16/06/2025</b>	A Emmett	<p>Section 6.4 – Updated guidance for updating software to introduce a 2-day pilot phase to minimise risk of a bad update causing a large-scale loss of service.</p> <p>Section 12 – New section Addressing Vulnerability Management</p> <p>Section 17 – New section outlining training managed by IT&amp;S and procedures for monitoring.</p>
<b>7/05/2026</b>	N Newell	<p>Academic Year updated 2025/2026</p> <p>Page 1 changed last reviewed date to May 2026</p> <p>5.5.3 added in Microsoft Intune reference</p> <p>Changed “day to day basis” to “daily basis” page 14</p> <p>Page 60, request for temporary removal of geographical restrictions – have increased this to 48 hours rather than the 24.</p>

## Appendix 2: ICT Systems Managers

<b>System Name</b>	
EBS	Head of Admissions and Information Services
Agresso	Head of Finance
Catalyst HR	Senior HR Business Partner Head of Finance
TMS	Head of Training Programmes & Apprenticeships
Web Services	Chief Technology Officer
Security Access System, Energy Management	Head of Estates, Facilities Management & Health and Safety
Cloud Services, including Identity, Security, E-mail, File Storage, Telephony & Web Portals/Sites	Chief Technology Officer
On Premise Infrastructure including Switches, Routers, Firewalls, Wi-Fi, Backup, Identity, Security & Server Workloads.	Chief Technology Officer
Telephony (Day to Day Operation)	Senior Customer Services Officer – Support Services
Library Systems (Booking and Catalogue)	Learning Resource Centre Manager

## **Appendix 3: Incident Report Form**

Form on next page



