SERC

INSPIRING. TRANSFORMING. ENRICHING.

SOP NUMBER: 206-10-2015

ACADEMIC YEAR: 2017/18 ONWARDS

DATE OF THIS ISSUE: OCTOBER 2017

TITLE:

ICT Systems and Services SOP

Summary of Contents:

ICT Services Procedures:

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

List of ICT Systems Managers

Date First Created:
30 September 2015

Last CMT Approval Date:
15 October 2015

Responsible Owner:

Head of ICT Infrastructure

(For Social Media content see Senior Marketing Officer)

REVIEW INFORMATION

Reviewed: October 2017

Next Review Due: March 2019

Requires CMT Approval (yes/no): Yes

Previous Reference (for control purposes):

155-05-2014 ICT Systems and Services SOP
189-06-2015: Social Media SOP

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

Date Procedure Screened – October 2016

1.0 Background

1.1 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.

1.2 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.

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

2.0 Scope

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

3.0 Summary of ICT Systems and Services Procedures

The following are set out below:

The Communication Plan and review information for this SOP can be found here

4.0 Access Control Procedure

4.1 Requirement for access controls

The business requirements for access controls on computer systems are:

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

4.2 Access Control Rules

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

Access Control Rules – System and Network Administrators
System and network administrators will be permitted the highest access levels to information within their information system or domain provided that:

- Such access is required to administer and manage the information system, information store or network domain.
- Strict observance of data confidentiality is practised.
- Strong passwords are selected as per guidelines issued in the College Password SOP.

4.3 Types of Access Control Employed

The type of access control that will be used include:

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.

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

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

Network Controls
Protection of the College network will be achieved by the use of firewalls, access control lists and where appropriate VLANS (Virtual Local Area Networks).

4.4 Monitoring and Review of Access

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

4.5 Reporting of Incidents

All users have a responsibility to report to appropriate system managers (see Appendix 1):

- 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.

Back to top

5.0 Malware – (viruses, ransomware, worms, trojan horses, spyware)

5.1 Introduction

The increased growth and dependence on ICT systems necessitates in appropriate support, security and contingency arrangements being 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

Definitions of Main Malware Types

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

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

5.2 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 ICT devices[1]. Furthermore, organisations who interchange information regularly between employees or indeed other organisations increase the likelihood of infection spreading.

5.3 Preventative Measures

The College uses a commercial anti-malware product that provides coverage for all servers, PCs and laptops. The product is updated on all servers and desktops directly when latest updates are available from the vendor's web site. Non-protected devices are proactively identified by the software permitting viral infection weaknesses to be exposed and dealt with. However, it is not acceptable to rely on the anti-malware product alone to prevent a viral outbreak. There are a number of mandatory stipulations to be observed by staff and students to ensure the risk of virus and spyware infections are kept to a minimum:-

- All Servers, PCs and laptops and other ICT devices[1] brought on to any College Centre must be properly configured for automatic updates and have up to date anti-malware software installed.
- It is not permissible to attempt the interrupting or disabling of automatic updates to the anti-malware software.
- All College–owned laptops and PCs must be connected to the College network at least once per week to facilitate anti-malware updates.
- Personally owned laptops and PCs must be kept updated with anti-malware software particularly if such devices are used to interchange information with College systems.
- It is not permissible to copy/upload any material to any device on the College network unless that device (i.e. PC or laptop) has the most recent anti-malware updates installed. Advice should be sought from the ICT Support Department if staff or students have any doubts as regards the integrity of data stored on portable media regardless of the media having been previously scanned.
- Only software procured and installed by the College may be used on any College owned ICT device. Installation and execution of any other type of software, including screensavers and games is prohibited.
- Use of peer to peer file sharing programs is strictly forbidden i.e., Kazaa, Limewire, Bear Share, due to the extremely high risk of virus introduction.
- Installation or use of spyware software is forbidden.
- It is not permissible to download any software from any spyware websites.
- Unexpected or suspect e-mail messages with or without attachments must be deleted immediately. Care must also be taken to immediately empty the Deleted Items folder.
- All users should monitor 'IT announcements' email for new virus or spyware alerts and take appropriate action.
- Downloading of any file type from unsolicited web sites is prohibited.
- It is the responsibility of all users of College computing facilities to ensure that data stored on portable devices (i.e. laptops, Macbooks, tablets) or portable media such as USB drives or Smart Phones is backed up.

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

- Suspected virus infections must be reported immediately to the ICT Support Department.

5.4 Levels of Protection

Having anti-malware protection on servers and desktops provides multi-level protection in that material sent via e-mail or the web is scanned on the e-mail/web server before being accessed by client PCs. Furthermore, material loaded via portable media[2] is scanned by the client PC and then scanned again by the anti-malware guarded file server.
All College servers including domain controllers, file servers, firewall and any other on premise services must be protected with anti-malware software.

Additional protective measures include:

- Certain file types known to “hide” or contain viruses are blocked if included in e-mail attachments. Some examples include: .exe, .vbs, .com, .mdb.
- Macro security levels In MS Office suite are set to Medium or High.
- Prevention of software installation on ICT devices by using Microsoft Windows group policies.
- Infected file attachments on external e-mail messages coming into the College are removed.
- Off-line content is deleted from PC/laptops after a successful login has taken place.

5.5 Reporting

Any indications of, or suspicions of virus or spyware activity must be reported to the Regional College ICT Support Section at one of the local campuses: Bangor, Downpatrick or Lisburn.

5.6 Dealing with a Malware outbreak

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

- Head of ICT Infrastructure to inform Heads of School and Unit Heads of scope and scale of infection.
- ICT staff will attempt to isolate infected device(s).
- If required, infected devices will be disconnected from the network.
- If required, unaffected network segments will be isolated from infected segments.
- Virus- free device with latest anti-malware software will be used as a cleaning medium for cleansing of infected files. If feasible, a secondary anti-malware product will be used to ensure that infected material and devices have been entirely cleansed.
- Upon removal of the infection, all servers and networked PCs, laptops will be updated with the latest anti-malware updates.
- The “all clear” to be issued by the Head of ICT Infrastructure to Heads of School and Unit Heads.
- An investigation to be initiated by the Head of ICT Infrastructure as to the cause of infection. On completion, a report is to be produced and forwarded to the Director of Curriculum and Information Services, outlining appropriate countermeasures and safeguards.

5.7 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. The College will initiate disciplinary action against any employee or student who either deliberately introduces, or attempts to introduce malware, or who is complicit with other parties or individuals in introducing or attempting to introduce a virus or spyware software.

5.8 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.

5.9 Additional Security Recommendations (Personal PCs/laptops)

Keep Windows Firewall turned on at all times. This will stop unwanted access to the computer on the Internet (especially at home).

Ensure that some form of antivirus and anti-spyware software is running and that it is updated at least on a daily basis.

Back to top

6.0 Email and Messaging Procedure

6.1 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.

6.2 Acceptable use of Email and Messaging

The following guidelines must be adhered to:

- Users may access only their own mailbox and must not use, or attempt to access another mailbox. It is not permissible to send e-mail from another College staff or students mailbox unless approval has been granted by both the mailbox owner and the sender's line manager.
- Users are discouraged from sending large file attachments to individual or multiple mailboxes to either internal or external recipients. "Large" can be defined as anything over 30MB.
- In order to reduce the risk of malware infection, users should not open file attachments of any file type unless:

  a. It is a Microsoft Office file (i.e. Word document, Excel spreadsheet) 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 delete dubious mail messages or check with ICT Support Department for advice (see Section 6.3 for more information).

- Users must not e-mail or message any illegal, malicious or copyright protected files or information.
- Users are not permitted to use the College email and messaging services as a medium to transmit offensive or abusive material or messages.
- Email should be used for SERC business; teaching or study-related activities provided such activities are legal.
- Email spamming is forbidden. (Spamming is the forwarding on, or sending of unwanted e-mail to other users or groups of users without their prior knowledge or consent). The mailing of multiple users, or multiple mailing groups, or the mailing of one user or mailing group many times is also considered as spamming.
- Phishing e-mails must not be created or forwarded to others. Furthermore, phishing e-mails received that request personal (including passwords or usernames), financial or other confidential or sensitive information should be deleted.
- Each user is responsible for managing the content of their mailbox. There is an expectation that each user will delete processed messages from Mailbox folders. SERC cannot guarantee the integrity and indefinite storage of mailbox information.
- E-mail can be set up and accessed on mobile devices such as mobile phones and tablet computers as long as the devices are secured in accordance with the terms of the Remote Access and Mobile Computing Standard Operating Procedure (SOP).
- All messages should be constructed observing acceptable etiquette. (For example, capital letters and large fonts should be avoided.)

6.3 Dealing with Dubious or Suspicious Emails

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

- Messages that contain malware. There 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, (phishing). There are messages that 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.
- 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”. (The authenticity of hoax mail can be checked with leading anti-malware software companies via their web sites).
- 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”.

6.4 Breach of guidelines

Please note that 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 have the right to check material stored on computing facilities if it is suspected that acceptable use has been violated.

6.5 Staff and Student Leavers

Final year students will have their mailboxes deleted twelve months after leaving the college. (Their computer accounts will expire on 30th September of the year they finish their course).

Full time staff that leave the College will have their e-mail accounts disabled for three months and then their mailbox will be deleted.

Back to top

7.0 Internet Use Procedure

7.1 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. Should anyone inadvertently access any offensive or sexually explicit material, they should leave that site immediately and inform both their Line Manager/course tutor and the ICT Support Section giving details of the URL visited.

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

7.2 Acceptable Internet Usage

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

7.3 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 attempt at 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 be avoided if possible. (Students and staff should use their College e-mail accounts).

7.4 Accessing and use of Social Media and Blogging Web Sites

The College will block access to social media sites for staff and students as a general rule. However, exceptions can be made for particular staff and student groups if it is deemed necessary for business or educational purposes - see Section 8: Social Media.

7.5 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 or students' tutor or Assistant of Head(s) 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.

Back to top

8.0 Social Media

8.1 Background

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

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

- Online social forums such as Twitter; Facebook; Google+, LinkedIn, Instagram and Snapchat
- Blogs, videos and image-sharing websites such as YouTube and Flickr
- Messaging technologies such as Skype for Business
- Personal web space

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

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

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

8.2 Scope

This applies to all staff employed, or third parties engaged by, or on behalf of SERC in relation to the use of social media for business, **whether it is in normal work time or not**, **on SERC or personal computing facilities and whether posting on social media using personal or work related accounts.**

8.3 Breach of Procedure

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

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

8.4 Use of Social Media at Work

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

Procedures for setting up social media for business purposes are set out in section 8.7. Staff must be aware at all times that, while contributing to the College's social media activities, they are representing SERC and should use the same safeguards as they would with any other form of communication.

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

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

- **Bring SERC into disrepute**, for example by:
  - presenting personal views as those of SERC;
  - criticising or arguing with customers, clients, colleagues, students or rivals;
  - making defamatory or libellous comments about individuals or other organisations or groups;
  - posting images without the correct consent, or that are inappropriate, or links to inappropriate content;
  - Edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work as the source of the correction will be recorded as the SERC IP address and will appear as if it comes from SERC itself.

- **Breach confidentiality legislation or codes of conduct**, for example by:

  - revealing confidential information owned by SERC;
  - giving away confidential information about an individual (such as a colleague, student, or customer contact) or organisation (such as a rival business); or
  - discussing SERC's internal workings (such as future business plans that have not been communicated to the public);

- **Breach copyright**, for example by:
  - using someone else's images or written content without permission; or
  - failing to give acknowledgement where permission has been given to reproduce something;

- **Breach data protection legislation**, for example by:
  - disclosing information about an individual without their consent;
  - allowing unauthorised access to the personal data held on a social media account on behalf of SERC; or
  - processing personal data in such a way that would breach Data Protection principles;

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

8.5 Personal Use of Social Media

SERC does not permit personal use of social media during working hours without prior permission.

While they are not officially acting on behalf of SERC, staff must be aware of the damage to the College if they are recognised as being employed, or engaged by SERC.
Any communications that staff made in a personal capacity through social media must not bring SERC into disrepute, breach confidentiality or copyright, breach data protection, or do anything which could be considered defamatory or discriminatory against any individual or organisation.

During personal use of social media, SERC staff must NOT:

- Use SERC email addresses and other official contact details for setting up, or communicating through, social media accounts.

- Identify themselves as SERC employees.

- Publish photographs, videos or any other types of image of SERC students on personal social media.

- Have contact with any SERC student, unless that student is a family member or pre-existing personal friend.

- Have contact with any student's family member if that contact specifically relates to SERC business, is likely to constitute a conflict of interest, or call into question the staff member's objectivity.

- Accept ‘friend requests’ from students; they should signpost students (during class time) to become ‘friends’ of one of the official SERC social media sites.

- On leaving SERC service, contact SERC students via personal social media sites. Similarly, current SERC staff must not contact students from any educational establishment they were previously employed at by means of personal social media unless that student is a family member.

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

Staff are strongly advised to ensure that they set the **privacy levels** of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff should keep their passwords confidential, change them often and be careful about what is posted online. It is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

8.6 Social Media Monitoring

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

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

The College reserves the right to restrict, deny or remove Internet access, or access to particular social media websites, to or from any employee.

8.7 Setting up Official SERC Social Media

There must be strong pedagogical or business reasons for creating official SERC social media sites to communicate with students or others. Staff should also refer to the Photographs and Video Involving Children and Vulnerable Adults SOP.

Advance permission must be obtained from Communications and Marketing before creating any new official SERC social media site.

To apply to set up an official SERC social media site:

- Complete the application form (Appendix 2) and submit to Communications and Marketing.
- If approved, the form at Appendix 3 must be completed and returned to Communications and Marketing.
- A 6 Month Review will be conducted of all presences (Appendix 4).
- Twitter and Facebook operational rules must be read and adhered to (Appendix 5) available here for separate download in pdf format.

Forms are available for download in Word format:
Social Media Presence Application Form
Social Media Presence Planning Checklist
6 Month Social Media Presence Review

Back to top

9.0 Network Management Procedure

9.1 Introduction

Purpose

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.

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

Definitions:

- Remote Access Devices; Any equipment capable of establishing a physical network connection with a device or network that is not owned or operated by the College.
- Network Components; Includes, but is not limited to: switches, routers, firewalls, interface converters, patch cables and data cabling, wall sockets, wireless access points, Remote Access Devices.
- End User Devices; PCs, Macs, Laptops, Macbooks, Servers, Workstations or other devices that are not performing the function of a Network Component.
- The College's Computer Network; All of the Colleges controlled Network Components that are directly or indirectly connected to the external JANET interface (or its replacement).
- The ICT Support Dept.; The body responsible for all activities pertaining to the Computer Network.

Procedure

- The College requires that only authorised persons shall manage and maintain the operation of the computer network.
- The ICT Support Dept. 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 ICT Support Dept. is responsible for the:
- Connection of any and all Network Components to the Computer Network. The ICT Support Dept. may, at its discretion, delegate specific activities to End User departments to support their activities as efficiently as possible.
- Configuration and management of all Network Components comprising the Computer Network.
- Management of all network based protocols (IP addresses, routing tables, DNS, DHCP, Routing protocols 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.
- The ICT Support Dept. will operate a Fault Reporting facility for the logging of all faults and problems with the Computer Network. All faults requiring the attention of the ICT Support Dept. must be logged. The ICT Support Dept. 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 ICT Support 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 ICT Support Dept.
- Requests for VPN (Virtual Private Network) access to the College Network for College staff must be approved by the Departmental Head and the Head of ICT Infrastructure.
- The College will provide remote access for staff and students to the College Intranet. It is incumbent upon each remote user to ensure that their remote devices are protected by updated anti-malware software.
- Requests for remote access to the College network or any College ICT System by third parties must be addressed to the Head of ICT Infrastructure for approval.
- Third party access to the College network must be via an agreed secure connection (e.g. VPN). The third party must inform the Head of ICT Infrastructure giving details of reason(s) for requiring access, the identity of the party or person accessing the network and the estimated duration of access.
- The third party shall inform the Head of ICT Infrastructure when the network access session is due to close. Confirmation of work carried out must be provided by the third party

9.1 Computer Accounts for Staff and Students

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

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

Back to top

10.0 Password Procedure

10.1 Introduction

Overview

Passwords are an important aspect of computer security. They are 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, as outlined below, to select and secure their password.

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.

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.

10.2 Procedures

- 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.

10.2 General Password Construction Guidelines

Poor, weak passwords have the following characteristics:

- The password contains less than seven characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word 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).

Strong passwords have the following characteristics:

- Contains both upper and lower case characters e.g. a-z, A-Z
- Have digits and punctuation characters as well as letters e.g. !@#£$%^&*()+-
- Must be at least 7 alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon etc.
- Passwords should never be written down or stored on-line. Attempts should be made to create passwords that are easy to remember. You could create a password on a song title, affirmation or other phrase. For example, the phrase might be: “This May Be One Way To Remember” could be a password of “TmB1w2R!”

10.3 Password Protection Standards

- Do not use the same password for SERC accounts as for other non SERC accounts such as personal e-mail accounts, Banking accounts, PIN numbers, or any other account. Where possible, don’t 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.

- Do not share SERC passwords with anyone, including administrative assistants or line managers. All passwords are to be treated as sensitive confidential SERC information. It is not permissible to:-
  - Reveal the password over the telephone to anyone (apart from password resets - see 10.5).
  - Reveal a password in a single e-mail message (apart from password resets – see 10.5)
  - Reveal a password to a manager.
  - Talk about a password in front of others.
  - Hint at the format of a password.
  - Reveal a password on questionnaires or security forms.
  - Share a password with family members.
  - Reveal a password to co-workers while on holiday.
- If someone demands a password, refer them to this document or have them call someone in the ICT Support department.
- Do not use the “Remember Password” feature of applications.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file or ANY computer system without encryption.
- Change passwords at least once every six months.

If you suspect your password has been compromised, report the incident to the ICT Support Department and change your password immediately.

10.4 Resetting Passwords

- All staff and students can reset their own passwords from a College PC/Mac or from the College Intranet remotely.
- All teaching staff can reset a student’s password by using the Student Lockout Wizard which is available on the College 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 a student to disclose their password.
- All ICT Support Staff can reset any other College student or staff member’s password. In both cases, suitable ID must be produced before the password can be reset. Staff and students should not request their password to be changed via e-mail or telephone unless the ICT Support Staff member can have good assurance of authenticity of the person requesting. The minimum requirement for establishing authenticity is to obtain the student/staff number, name, department/course of study, or name of another person in the same class or department, tutor name (in case of student request). Upon establishment of authenticity, the password can be disclosed as long as:
  - The password is broken into 2 parts and transmitted in two separate e-mails.
  - The password is supplied by the caller to the ICT Support staff and not vice-versa
  - The “User must change password at next login” attribute must be set by the ICT Staff member on the user account.

10.5 Enforcement

Password “cracking” or guessing may be performed on a periodic or random basis by ICT department staff. If a password is guessed or “cracked”, the user will be required to change it.

Any member of staff or student found to have violated this procedure may be subject to appropriate disciplinary action.

Back to top

11.0 ICT Security Controls and Incident Procedure

11.1 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.

11.2 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 role of the Security Management Group (SMG) 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 in the College of major security policy decisions and plans for implementation. Should a security incident occur, the SMG will have authority to scrutinize the results of log file monitoring.

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 Security Management Group.

System Controls

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

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

Physical Controls

Controls such as secured areas for location of key ICT items will be provided.
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.

11.2 Security - Good Practice Guidelines

Security Good Practice – DOs

- Lock workstations whilst left unattended.
- Report suspicious behaviour or persons acting suspiciously
- Bring laptops in weekly to connect to the College network for anti-malware and Windows updates
- Check that your PC/laptop has up-to-date anti-malware software installed.
- Change your password when prompted to do so.

Security Good Practice - DON'Ts

- 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 PCs, Macs, MacBooks or laptops unless the drives are encrypted
- Attach any device to the College network unless authorised to do so.

11.3 Procedure for reporting a security incident or security vulnerability

- Contact the appropriate Data Owner immediately.
- In conjunction with the Data Owner, complete an incident report
- Remedial action to be taken by the Data Owner (where possible) and SMG 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 Head of ICT Infrastructure to reduce the risk of a further security incident occurring. This arrangement will be in force until a permanent solution is implemented.

11.4 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 Head of ICT Infrastructure and the Security Management Group. 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).

11.5 Links with other bodies

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

11.6 Responsibility

CMT, through the SMG, 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.

Back to top

12.0 Software Licensing Management Procedure

12.1 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.

12.2 Access

In order to prevent installation of unlicensed software, only ICT Support staff have the necessary access to install software.

Access is granted to the following:

- PCs, laptops, Macs and MacBooks – all ICT Support Staff – (depending upon the method – see Section 12.3. Method of Installation**)**.
- Servers – Senior ICT Support staff only.

- Apple Macs – The technical support staff who work for the Schools of Computing and Media and the School of Performing Arts.

12.3 Method of Installation

There are two main methods of software installation:

- Deployment – Only ICT Support staff are permitted to deploy or authorise deployment of packaged software.
- Manual Installation – Only ICT Support 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 Head of ICT Infrastructure.

(Software Installation Procedure provides details for ICT Support staff on installation of software)

12.4 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 Head of ICT Infrastructure by the Departmental Head or Head of School for licensing confirmation.
- Installation authorisation to be granted by Head of ICT Infrastructure to appropriate ICT technical staff.

12.5 Control

All staff and students (other than groupings stated above in Section 12.2) 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 software.

12.6 Procurement and Recording

Procurement of application software must be carried out by the Head of ICT Infrastructure.

Back to top

13.0 Data Management Procedure

13.1 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.

13.2 Definitions 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, data will be classified into two main categories:-

- Personal, Confidential and Sensitive data
- Other data

Personal, Confidential and Sensitive data
‘Personal’ can be defined as:-

- Any information containing names **and including** any, or all of the following:-
  Dates of birth, addresses, postcodes, financial details such as banking details, medical details or histories and photographic images.

‘Confidential’ can be defined as:

- Any business information that is classified as “confidential”
- 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
- Any security information such as system passwords, user account details.

‘Sensitive’ can be defined as:

- Any information relating to medical, financial, criminal or sexual orientation circumstances.

Other data
‘Other data’ includes any other stored data which does not fall into the ‘Confidential’, ‘Sensitive’ and ‘Personal’ category.

13.3 Management of Electronic Data – Both Classifications

Storage and Transmission of Data

- Source data must be stored securely on College-secured storage media such as shared drives on College servers or on the College-provisioned Office 365 OneDrive.
- Source or copy data of personal, sensitive or confidential type must not be stored on any external hosted service such as Dropbox, Google Docs or Evernote or any other similar storage service. The only approved external hosted storage service is Office 365 OneDrive. (This has the Government G-Cloud approval for storage for personal, confidential and sensitive information).
- Copies of ‘other data’ 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 source data regarded as personal, sensitive or confidential must only be taken and transported by portable media as long as:
  - Approval has been sought from Head of School, Unit Head or Director of the specific department or unit.
  - That the method of transportation is deemed secure. Personal, sensitive or confidential data must be transported in encrypted media such as encrypted USB pens, or on encrypted hard drives, or on College-owned laptops that have encrypted hard drives, or any other approved secure media.
  - Great care is taken not to lose or mislay the storage device.
- Secure means of transmission of data must be used (e.g. transmission via secure internet connection with College approved encryption algorithm). Data must not be transmitted by unencrypted e-mail messages, instant messaging or any other insecure means or media.

- It is not permissible to store personal, sensitive or confidential data on:
  - Personally owned devices such as PCs, laptops, MacBooks, tablets or mobile phones
  - Any storage medium, (personal or College provided), if that has not been encrypted. This includes memory sticks, hard drives, camera cards, DVDs and any other storage media

Retention of data storage

- The College will retain data records in accordance with statutory obligations.
- The College will remove mailboxes and data created by students as part of their course within 12 months after the conclusion of the course. Students wishing to retain any of their course work may do so before finishing their course and if prior consent has been given by their tutor.
- Student accounts will expire on the 30th of September after completion of their course of study.
- Staff who are leaving College employment are advised to clear out their personal storage and mailboxes before their last day of employment. Staff should pass on information that could still be required by the College to their Line Manager. This could include exam results, course work or financial or business information.
- Upon receipt of notification from the Human Resources department of staff having ceased employment, staff network login accounts will be disabled. All data and mailbox contents stored against a disabled account will be deleted after a three month period.
- The College will not be responsible for loss of data created by staff members or students upon their ceasing their course of study or employment with the College.

Backup

- The College will endeavour to backup and store on and off-site all corporate data. 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.
- 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 (e.g. updating of documents or folders must be uploaded to the area where source information was stored, or if new copy was created, it must be uploaded to the appropriate storage area

that the author has access to. Version control measures must be employed. See Mobile and Remote Computing Procedure).

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. 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 contacting the ICT Support 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 PC/laptop/AppleMac/tablet used is secured with the latest anti-malware software and that virus definitions are continually kept updated.
- Passwords are not disclosed to third parties and that third parties are not permitted to access College services using the staff or students member's 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".

13.4 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. Accounts can only be setup upon notification from Human Resources Department that all appropriate checks and controls have been completed (this includes signing of Acceptable Use Policy). Passwords must comply with the College password procedure

Version Control
Manipulation of copied data incurs risk of partially updated copies of the source documents or files. On-line editing reduces greatly the risk of multiple copies of partially edited or 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"

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 the College anti-malware procedure for further details on virus control)

13.5 Asset and Inventory Management

All items 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).

13.6 **Access to Data**

Departmental Shared Drives (Staff Resources (S Drive) and Team Sites
Requests for access to above should be made via the Fault/Request 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 Staff Resources folders will be processed by the.
Requests for Teamsite access will be processed by the MILT Development Team.

Requests to access another staff member's personal drive, OneDrive or mailbox.
Each staff member / student have 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 Head of ICT Infrastructure as regards arranging to access the drive/mailbox. The access must be witnessed by the Head of School/Head of Unit and by Head of ICT Infrastructure or a senior member of the ICT Infrastructure department (Band 5 or above).

- A staff member is on extended period of absence due to illness or annual leave. Access to the staff drive/mailbox will be granted in urgent cases only if the request is made by the Head of School/Head of Unit indicating the reasons for requiring access to the Head of ICT Infrastructure 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 Head of ICT Infrastructure. As stated above, the access must be witnessed by Head of ICT Infrastructure, or a senior member of the ICT Infrastructure department. The access will only be for a duration long enough to obtain the necessary information and whilst witnessed as stated above. Browsing of the personal drive or mailbox for information other than the required information is forbidden. Once the required information has been located, the access will be removed. The required information is not to be copied or forwarded on, unless the staff member has authorised that.
- If for various reasons, the matter is regarded as most urgent and the staff member's approval cannot be obtained, the matter must be referred to the Chief Human Resources Officer for deliberation.
- Members of the ICT Infrastructure section 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.

13.7 **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 ICT Support Section 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 Director of Curriculum and Information Services, or a member of the College's Senior Management Team (SMT), who will then contact the PSNI.

13.8 Disclosure of Information

It is not permissible for any College information, or any information contained in any College information system to be disclosed for purposes of offering competitive advantage to any third party. It is also not permissible for any staff member to use any information to further any independent or private business venture.

13.9 Good Practice Guide on Data Management and ICT Security

SERC must ensure that personal data of students, colleagues and visitors is treated with appropriate security measures by all who handle it. Principle 7 of the Data Protection Act (1998) states:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

With so much 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. Personal data is stored by the College in both paper and electronic format.

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

PASSWORD SECURITY

ALWAYS…..

- Create strong passwords which are easy for you to remember and impossible for someone else to guess.
- Strong passwords should be at least 7 characters long with a combination of letters, numbers upper/lower case and even symbols such as @*!£&$
- Change password at regular intervals

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 personal/confidential/sensitive information on secure College storage systems i.e. teamsites/network drives.
- Lock your PC/Mac whilst unattended – 'Ctrl + Alt + Del +"Lock this computer".
- Lock classrooms and 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 ICT 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 personal/confidential/sensitive information on an unsecured mobile device such as a USB pen, personal or third party PC, Mac, laptop, MacBook or external hard drives.
- Store personal/confidential/sensitive information on a personal mobile phone.
- Store personal/confidential/sensitive information on a third party storage facility such as Google Docs, Dropbox, Evernote – we cannot guarantee their security. The exception to this will be Office 365 OneDrive.
- Use your personal email account for SERC related business - we cannot guarantee their security.
- Allow anyone to use your PC/Mac, MacBook, laptop or tablet whilst you are logged in – you are responsible for processing carried out under your name.
- Provide personal details of yourself or others to unauthorised third parties.
- Respond to web links requesting personal details of yourself or others.
- Do not have liquids close to your device in case of spillage.

'SERC' HANDHELD AND PORTABLE ELECTRONIC STORAGE DEVICE SECURITY (E.G MOBILES, LAPTOPS, MEMORY STICKS ETC)

ALWAYS…..

- Guard your mobile device (i.e. mobile, 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 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 to access the College's personal data sets to ensure that those data, whether held electronically or manually, are kept securely and not disclosed unlawfully, in accordance with the College's Data Protection Policy and the Data Protection Act 1998. 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 £500,000 for serious breaches of the Data Protection Act (1998).

Back to top

14.0 Remote Access and Mobile Computing Procedures (including Bring Your Own Device)

14.1 Introduction

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

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

14.2 Mobile Computing

Categories of portable devices include:-

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

(The above is not a prescriptive list)

Working with portable media and devices

The following guidelines should be adhered to:

- Personal, sensitive or confidential information should not be stored on any portable device unless that device supports encryption and has been approved for use by a College authority such as Head of ICT Infrastructure.
- Only encrypted devices should be used for storage of personal or confidential data.
- Persons using portable media must ensure that devices are not left unattended in public places.
- Portable devices must be adequately secured (e.g. laptops are not left logged on).
- Loss of portable devices must be immediately reported to the staff member's Unit Head or Head of School, or student's lecturer (in case of students). If it has been established that personal or confidential data has been stored on the stolen device, the incident will be escalated to the Security Management Group (SMG). (Please refer to Security and Incident Procedure).
- College owned laptops must be connected to the College network at least once per week for anti-malware, application and operating system updates.
- College owned laptops must have data encryption enabled on the local hard drive. (This is dependent upon hardware capability to support encryption method).
- College provided mobile phones with messaging capability must have a pin number or password set on the handset.

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

14.3 Data Control and Authority

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

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

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

- preventing theft and loss of data,
- where appropriate keeping information confidential and
- maintaining the integrity of data and information.

Staff members should:

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

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

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

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

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

14.3 Remote Computing

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

Working from a remote location
The College will provide a secure connection for remote access such as SSL (Secure Sockets Layer), VPN (Virtual Private Network), or other secure method.
The following guidelines should be adhered to when working from a remote location in terms of accessing College ICT systems:-

- Devices used from a remote location must have updated anti-malware software installed.

- Only College staff will be permitted to access College ICT systems from remote locations. Third parties are not permitted to access College systems from a College staff or student member’s user account. It is incumbent upon staff and students to ensure that they do not disclose password details to any third party and that they ensure that they have logged off from the College system and remote device before leaving the same device.

- Any files to be copied to a College storage area must be malware checked in first instance by the person wishing to copy or upload the file. Infected files must not be copied.
- It is not permitted to copy large files from a remote location to a College server unless prior consent from the ICT Support section has been granted. File compression utilities should be used on any file over 20MB (megabytes) in size.

14.4 General Guidelines

Version Control
Due care must be taken when working remotely or with copies of source documents on portable media that appropriate version control takes place. It is recommended that copy documents have a version number appended to the file name (e.g. mobilecomptungVer1.doc). Each document should also have a date of revision, author and name added to the document footer. The source document should only be overwritten with the approved version. Approval should be sought from Departmental Heads in situations where documents are to be copied to shared departmental drives.

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

Use of Third Party Devices
Users of third party devices requiring networking connectivity other than via the wireless network, must seek prior permission from the ICT Support Department.

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

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

Back to top

15.0 Communication Plan

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

16.0 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).

Back to top

Appendix 1

ICT Systems Managers

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

Back to Reporting of Incidents

Appendix 2

Social Media Appendix A

Application to Create a Social Media Presence

Staff Name: ………………..……………………………

School/Department: ……………………………………

Email address: ……………………………..……….. Date of Application: ……………………..

Completed application forms should be emailed to Communications and Marketing at otumelty@serc.ac.uk for approval.

You will be notified of the application outcome and, if approved, will be asked to complete and return the Social Presence Application Checklist (Appendix B).

Please answer these questions as fully as possible

Who is the page designed to represent? *School or Department etc.*	
Is your Head of School aware? *Do you have approval to proceed?*	
Which social presences are you requesting? *Facebook, Twitter etc.*	
Who is your target audience? *Demographics (Age, Gender), Location etc.*	
What is the objective of the presence? *Student Recruitment, Information etc.*	
Have you had any feedback from students or other stakeholders about creating a new communications channel? *Are students using their own for College purposes etc.?*	
How will you measure success of the presence? *Followers, Engagement, Reach Recruitment etc.*	

How do you plan to create a calendar of engaging, informative and entertaining posts? *What resources will you use? Such as awareness days, college related events etc.*	
Is there a similar presence outside SERC? *Are there any pages like yours, which you may wish to model?*	
What resources do you have available to monitor the presence and respond to enquiries etc. *Do you have more than one person available to assist?*	
What safety concerns do you anticipate? *Use of Images, Bullying, Malicious Comments etc.*	
How will you mitigate against these? *SERC Policies such as the Photographs and Video Involving Children and Vulnerable Adults SOP*	

Back to Social Media

Appendix 3

Social Media Appendix B

SERC
INSPIRING. TRANSFORMING. ENRICHING.

Social Media Presence Planning Checklist

Staff Name: ………………..……………………………

School/Department: ……………………………………

Email address: …………………………………………. Date: …………………………………

This Planning Checklist should only be completed once you have been notified of a successful application. Completed forms should be emailed to Communications and Marketing: otumelty@serc.ac.uk

A 6 Month Review will be conducted of all presences (Appendix C)

Please answer these questions as fully as possible

What do you wish to call your presence? *What name will your presence go by, such as SERC Hospitality or SERC Travel and Tourism*	
Identify all members of your Social Media Team *Clearly state all the individuals in charge, their role (on the team), their email and mobile phone numbers.*	
How often are you planning to update the page? *Typically on average pages are updated 3 times a week.*	
How will the account be policed at the weekends? *Accounts can easily be temporarily shut down.*	
Will the account remain active during extended holidays? *Accounts can easily be temporarily shut down.*	
What will your policy be on seeking approval before posting (if necessary)?	
Have all of your Social Media Team read and understood the	

Facebook and Twitter Terms & Conditions? *These can be Located at Appendix D*	
Have all the Social Media Team read the Social Media SOP? *This is available online via the Learning Engine on the SERC Intranet.*	
Have you asked your target audience for feedback on your intentions? *What has the feedback been?*	
How do you intend to publicise your social media presence? *Traditional marketing, email etc.?*	
Have you signed your Social Media Team up to a Social Media training course? *These are available from Marketing and Communications.*	
Do you have a budget for any advertising on your social media channel? *Perhaps to increase your followers or promote recruitment?*	

Required Setup Information

Write a few sentences to tell people what your account is about.	
Do you want to link to a website which your page relates to, please supply details? *Such as a SERC course descriptor*	
Please attach one or more profile and cover pictures.	
If you are using Facebook they can promote your page to your target demographic. *Please supply what age range, gender and sorts of interests your demographic may have.*	

Please supply the following (where appropriate): *Address* *Enter hours of operation* *Short Description* *Course* *Phone* *Enter your email address* *Enter your website*	

Back to Social Media

Appendix 4

Social Media Appendix C

INSPIRING. TRANSFORMING. ENRICHING.

6 Month Social Media Presence Review

When a new social media presence is created, there will be a 2 month review in the below format and then, going forward a 6 month review will take place.

Name of Social Presence: ………………..……………………………

Staff Name: ……………………………………………………………..

School/Department: ……………………………………

Email address: ………………………………………… Date: ……………………………..

Completed forms should be emailed to Communications and Marketing: otumelty@serc.ac.uk

Please answer these questions as fully as possible. This will form the basis of a discussion.

What has your average reach been? *Available in Insights*	
What has your average engagement been? *Available in Insights*	
Please report follower growth? *Available in Insights*	
On average how many times are you posting per week?	
Please list high points. *Activities that have performed particularly well.*	
Please list low points. *Any negative experiences?*	
How has the presence performed against your expectations?	
Do you have a different strategy for the next six months?	

Back to Social Media

Social Media Appendix D

INSPIRING. TRANSFORMING. ENRICHING.

Social Media Terms & Conditions (UK)

Facebook

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement," "Terms," or "SRR") derives from the Facebook Principles, and is our terms of service that governs our relationship with users and others who interact with Facebook, as well as Facebook brands, products and services, which we call the "Facebook Services" or "Services". By using or accessing the Facebook Services, you agree to this Statement, as updated from time to time in accordance with Section 13 below. Additionally, you will find resources at the end of this document that help you understand how Facebook works.

Because Facebook provides a wide range of Services, we may ask you to review and accept supplemental terms that apply to your interaction with a specific app, product, or service. To the extent those supplemental terms conflict with this SRR, the supplemental terms associated with the app, product, or service govern with respect to your use of such app, product or service to the extent of the conflict.

1. **Privacy**

   Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions.

2. **Sharing Your Content and Information**

   You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

   1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
   2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
   3. When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how

you can control what information other people may share with applications, read our Data Policy and Platform Page.)

4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use your feedback or suggestions without any obligation to compensate you for them (just as you have no obligation to offer them).

3. Safety

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:

1. You will not post unauthorised commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
10. You will not do anything that could disable, overburden, or impair the proper working or appearance of Facebook, such as a denial of service attack or interference with page rendering or other Facebook functionality.
11. You will not facilitate or encourage any violations of this Statement or our policies.

4. Registration and Account Security

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.

2. You will not create more than one personal account.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal timeline primarily for your own commercial gain, and will use a Facebook Page for such purposes.
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any Page or application you administer) to anyone without first getting our written permission.
10. If you select a username or similar identifier for your account or Page, we reserve the right to remove or reclaim it if we believe it is appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. Protecting Other People's Rights

We respect other people's rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.
3. We provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.
4. If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or Trademarks or any confusingly similar marks, except as expressly permitted by our Brand Usage Guidelines or with our prior written permission.
7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone's identification documents or sensitive financial information on Facebook.
9. You will not tag users or send email invitations to non-users without their consent. Facebook offers social reporting tools to enable users to provide feedback about tagging.

6. **Mobile and Other Devices**

    1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging and data charges, will still apply.
    2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
    3. You provide consent and all rights necessary to enable users to sync (including through an application) their devices with any information that is visible to them on Facebook.

7. **Payments**

    If you make a payment on Facebook, you agree to our Payments Terms unless it is stated that other terms apply.

8. **Special Provisions Applicable to Developers/Operators of Applications and Websites**

    If you are a developer or operator of a Platform application or website or if you use Social Plugins, you must comply with the Facebook Platform Policy.

9. **About Advertisements and Other Commercial Content Served or Enhanced by Facebook**

    Our goal is to deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers. In order to help us do that, you agree to the following:

    1. You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.
    2. We do not give your content or information to advertisers without your consent.
    3. You understand that we may not always identify paid services and communications as such.

10. **Special Provisions Applicable to Advertisers**

    If you use our self-service advertising creation interfaces for creation, submission and/or delivery of any advertising or other commercial or sponsored activity or content (collectively, the “Self-Serve Ad Interfaces”), you agree to our Self-Serve Ad Terms. In addition, your advertising or other commercial or sponsored activity or content placed on Facebook or our publisher network will comply with our Advertising Guidelines.

11. **Special Provisions Applicable to Pages**

    If you create or administer a Page on Facebook, or run a promotion or an offer from your

Page, you agree to our Pages Terms.

12. Special Provisions Applicable to Software

1. If you download or use our software, such as a stand-alone software product, an app, or a browser plugin, you agree that from time to time, the software may download and install upgrades, updates and additional features from us in order to improve, enhance, and further develop the software.
2. You will not modify, create derivative works of, decompile, or otherwise attempt to extract source code from us, unless you are expressly permitted to do so under an open source license, or we give you express written permission.

13. Amendments

1. We'll notify you before we make changes to these terms and give you the opportunity to review and comment on the revised terms before continuing to use our Services.
2. If we make changes to policies, guidelines or other terms referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.
3. Your continued use of the Facebook Services, following notice of the changes to our terms, policies or guidelines, constitutes your acceptance of our amended terms, policies or guidelines.

14. Termination

If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 9.3, and 14-18.

15. Disputes

1. You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions.
2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim. Although we provide rules for user conduct, we do not control or direct users' actions on Facebook and are not responsible for the content or information users transmit or share on Facebook. We are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content or information

you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, of any user of Facebook.

3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR. WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

16. **Special Provisions Applicable to Users Outside the United States**

We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States:

1. You consent to having your personal data transferred to and processed in the United States.
2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website. You will not use Facebook if you are prohibited from receiving products, services, or software originating from the United States.
3. Certain specific terms that apply only for German users are available here.

17. **Definitions**

1. By "Facebook" or" Facebook Services" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; (c) social plugins such as the Like button, the Share button and other similar offerings; and (d) other media, brands, products, services, software (such as a toolbar), devices, or networks now existing or later developed. Facebook reserves the right to designate, in its sole discretion, that certain of our brands, products, or services are governed by separate terms and not this SRR.
2. By "Platform" we mean a set of APIs and services (such as content) that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
3. By "information" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook.
4. By "content" we mean anything you or other users post, provide or share using Facebook Services.
5. By "data" or "user data" or "user's data" we mean any data, including a user's content or information that you or third parties can retrieve from Facebook or provide to Facebook through Platform.
6. By "post" we mean post on Facebook or otherwise make available by using Facebook.
7. By "use" we mean use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
8. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives or has received data from us. If you no longer access Platform but have not deleted all data from us, the term application will apply until you delete the data.
9. By "Trademarks" we mean the list of trademarks provided here.

18. **Other**

1. If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to "us," "we," and "our" mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
2. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
3. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
4. If we fail to enforce any of this Statement, it will not be considered a waiver.
5. Any amendment to or waiver of this Statement must be made in writing and signed by us.
6. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.

7. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
8. Nothing in this Statement shall prevent us from complying with the law.
9. This Statement does not confer any third party beneficiary rights.
10. We reserve all rights not expressly granted to you.
11. You will comply with all applicable laws when using or accessing Facebook.

By using or accessing Facebook Services, you agree that we can collect and use such content and information in accordance with the Data Policy as amended from time to time. You may also want to review the following documents, which provide additional information about your use of Facebook:

- Payment Terms: These additional terms apply to all payments made on or through Facebook, unless it is stated that other terms apply.
- Platform Page: This page helps you better understand what happens when you add a third-party application or use Facebook Connect, including how they may access and use your data.
- Facebook Platform Policies: These guidelines outline the policies that apply to applications, including Connect sites.
- Advertising Guidelines: These guidelines outline the policies that apply to advertisements placed on Facebook.
- Self-Serve Ad Terms: These terms apply when you use the Self-Serve Ad Interfaces to create, submit, or deliver any advertising or other commercial or sponsored activity or content.
- Promotions Guidelines: These guidelines outline the policies that apply if you offer contests, sweepstakes, and other types of promotions on Facebook.
- Facebook Brand Resources: These guidelines outline the policies that apply to use of Facebook trademarks, logos and screenshots.
- How to Report Claims of Intellectual Property Infringement
- Pages Terms: These guidelines apply to your use of Facebook Pages.
- Community Standards: These guidelines outline our expectations regarding the content you post to Facebook and your activity on Facebook.

To access the Statement of Rights and Responsibilities in several different languages, change the language setting for your Facebook session by clicking on the language link in the left corner of most pages. If the Statement is not available in the language you select, we will default to the English version.

Twitter

- These Terms of Service (“Terms”) govern your access to and use of our Services, including our various websites, SMS, APIs, email notifications, applications, buttons, widgets, ads, commerce services (the “Twitter Services”), and our other covered services that link to these Terms (collectively, the “Services”), and any information, text, graphics, photos or other materials uploaded, downloaded or appearing on the Services (collectively referred to as “Content”). Your access to and use of the Services are conditioned on your acceptance of and compliance with these Terms. By accessing or using the Services you agree to be bound by these Terms.

1. Basic Terms
   - You are responsible for your use of the Services, for any Content you post to the Services, and for any consequences thereof. Most Content you submit, post, or display through the Twitter Services is public by default and will be able to be viewed by other users and through third party services and websites. Learn more here, and go to the account settings page to control who sees your Content. You should only provide Content that you are comfortable sharing with others under these Terms.

   - Tip: What you say on the Twitter Services may be viewed all around the world instantly. You are what you Tweet!

   - You may use the Services only if you can form a binding contract with Twitter and are not a person barred from receiving services under the laws of the United States or other applicable jurisdiction. If you are accepting these Terms and using the Services on behalf of a company, organisation, government, or other legal entity, you represent and warrant that you are authorised to do so. You may use the Services only in compliance with these Terms and all applicable local, state, national, and international laws, rules and regulations.

   - The Services that Twitter provides are always evolving and the form and nature of the Services that Twitter provides may change from time to time without prior notice to you. In addition, Twitter may stop (permanently or temporarily) providing the Services (or any features within the Services) to you or to users generally and may not be able to provide you with prior notice. We also retain the right to create limits on use and storage at our sole discretion at any time without prior notice to you.

   - The Services may include advertisements, which may be targeted to the Content or information on the Services, queries made through the Services, or any other information. The types and extent of advertising by Twitter on the Services are subject to change. In consideration for Twitter granting you access to and use of the Services, you agree that Twitter and its third party providers and partners may place such advertising on the Services or in connection with the display of Content or information from the Services whether submitted by you or others.

2. Privacy
   - Any information that you or other users provide to Twitter is subject to our Privacy Policy, which governs our collection and use of your information. You understand that through your use of the Services you consent to the collection and use (as set forth in the Privacy Policy) of this information, including the transfer of this information to the United States, Ireland, and/or other countries for storage, processing and use by Twitter. As part of providing you the Services, we may need to provide you with certain communications, such as service announcements and administrative messages. These communications are considered part of the Services and your account, which you may not be able to opt-out from receiving.

   - Tip: You can control most communications from the Twitter Services, including notifications about activity related to you, your Tweets, Retweets, and network, and updates from Twitter. Please see your settings for email and mobile notifications for more.

3. Passwords
   - You are responsible for safeguarding the password that you use to access the Services and for any activities or actions under your password. We encourage you to use “strong” passwords (passwords that use a combination of upper and lower case letters, numbers and symbols) with your account. Twitter cannot and will not be liable for any loss or damage arising from your failure to comply with the above.

4. Content on the Services

- All Content, whether publicly posted or privately transmitted, is the sole responsibility of the person who originated such Content. We may not monitor or control the Content posted via the Services and, we cannot take responsibility for such Content. Any use or reliance on any Content or materials posted via the Services or obtained by you through the Services is at your own risk.
- We do not endorse, support, represent or guarantee the completeness, truthfulness, accuracy, or reliability of any Content or communications posted via the Services or endorse any opinions expressed via the Services. You understand that by using the Services, you may be exposed to Content that might be offensive, harmful, inaccurate or otherwise inappropriate, or in some cases, postings that have been mislabeled or are otherwise deceptive. Under no circumstances will Twitter be liable in any way for any Content, including, but not limited to, any errors or omissions in any Content, or any loss or damage of any kind incurred as a result of the use of any Content posted, emailed, transmitted or otherwise made available via the Services or broadcast elsewhere.

5. Your Rights

- You retain your rights to any Content you submit, post or display on or through the Services. By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).
- Tip: This license is you authorizing us to make your Tweets on the Twitter Services available to the rest of the world and to let others do the same.
- You agree that this license includes the right for Twitter to provide, promote, and improve the Services and to make Content submitted to or through the Services available to other companies, organisations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such Content on other media and services, subject to our terms and conditions for such Content use.
- Tip: Twitter has an evolving set of rules for how ecosystem partners can interact with your Content on the Twitter Services. These rules exist to enable an open ecosystem with your rights in mind. But what’s yours is yours – you own your Content (and your photos are part of that Content).
- Such additional uses by Twitter, or other companies, organisations or individuals who partner with Twitter, may be made with no compensation paid to you with respect to the Content that you submit, post, transmit or otherwise make available through the Services.
- We may modify or adapt your Content in order to transmit, display or distribute it over computer networks and in various media and/or make changes to your Content as are necessary to conform and adapt that Content to any requirements or limitations of any networks, devices, services or media.
- You are responsible for your use of the Services, for any Content you provide, and for any consequences thereof, including the use of your Content by other users and our third party partners. You understand that your Content may be syndicated, broadcast, distributed, or published by our partners and if you do not have the right to submit Content for such use, it may subject you to liability. Twitter will not be responsible or liable for any use of your Content by Twitter in accordance with these Terms. You represent and warrant that you have all the rights, power and authority necessary to grant the rights granted herein to any Content that you submit.

6. Your License To Use the Services

- Twitter gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software that is provided to you by Twitter as part of the Services. This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Twitter, in the manner permitted by these Terms.

7. Twitter Rights

- All right, title, and interest in and to the Services (excluding Content provided by users) are and will remain the exclusive property of Twitter and its licensors. The Services are protected by copyright, trademark, and other laws of both the United States and foreign countries. Nothing in the Terms gives you a right to use the Twitter name or any of the Twitter trademarks, logos, domain names, and other distinctive brand features. Any feedback, comments, or suggestions you may provide regarding Twitter, or the Services is entirely voluntary and we will be free to use such feedback, comments or suggestions as we see fit and without any obligation to you.

8. Restrictions on Content and Use of the Services

- Please review the Twitter Rules (which are part of these Terms) to better understand what is prohibited on the Twitter Services. We reserve the right at all times (but will not have an obligation) to remove or refuse to distribute any Content on the Services, to suspend or terminate users, and to reclaim usernames without liability to you. We also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public.

- Tip: Twitter does not disclose personally identifying information to third parties except in accordance with our Privacy Policy.

- Except as permitted through the Twitter Services, these Terms, or the terms provided on dev.twitter.com, you have to use the Twitter API if you want to reproduce, modify, create derivative works, distribute, sell, transfer, publicly display, publicly perform, transmit, or otherwise use the Twitter Services or Content on the Twitter Services.

- Tip: We encourage and permit broad re-use of Content on the Twitter Services. The Twitter API exists to enable this.

- If you use commerce features of the Twitter Services that require credit or debit card information, such as our Buy Now feature, you agree to our Twitter Commerce Terms.

- You may not do any of the following while accessing or using the Services: (i) access, tamper with, or use non-public areas of the Services, Twitter's computer systems, or the technical delivery systems of Twitter's providers; (ii) probe, scan, or test the vulnerability of any system or network or breach or circumvent any security or authentication measures; (iii) access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by Twitter (and only pursuant to the applicable terms and conditions), unless you have been specifically allowed to do so in a separate agreement with Twitter (NOTE: crawling the Services is permissible if done in accordance with the provisions of the robots.txt file, however, scraping the Services without the prior consent of Twitter is expressly prohibited); (iv) forge any TCP/IP packet header or any part of the header information in any email or posting, or in any way use the Services to send altered, deceptive or false source-identifying information; or (v) interfere with, or disrupt, (or attempt to do so), the access of any user, host or network, including, without limitation, sending a virus, overloading, flooding, spamming, mail-bombing the Services, or by scripting the creation of Content in such a manner as to interfere with or create an undue burden on the Services.

9. Copyright Policy

- Twitter respects the intellectual property rights of others and expects users of the Services to do the same. We will respond to notices of alleged copyright infringement that comply with applicable law and are properly provided to us. If you believe that your Content has been copied in a way that constitutes copyright infringement, please provide us with the following information: (i) a physical or electronic signature of the copyright owner or a person authorised to act on their behalf; (ii) identification of the copyrighted work claimed to have been infringed; (iii) identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit us to locate the material; (iv) your contact information, including your address, telephone number, and an email address; (v) a statement by you that you have a good faith belief that use of the material in the manner complained of is not authorised by the copyright owner, its agent, or the law; and (vi) a statement that the information in the notification is accurate, and, under penalty of perjury, that you are authorised to act on behalf of the copyright owner.

- We reserve the right to remove Content alleged to be infringing without prior notice, at our sole discretion, and without liability to you. In appropriate circumstances, Twitter will also terminate a user's account if the user is determined to be a repeat infringer. Under the U.S. Digital Millennium Copyright Act, our designated copyright agent for notice of alleged copyright infringement appearing on the Services is:
  Twitter, Inc.
  Attn: Copyright Agent
  1355 Market Street, Suite 900
  San Francisco, CA 94103
  Reports: https://support.twitter.com/forms/dmca
  Email: copyright@twitter.com

10. Ending These Terms

- The Terms will continue to apply until terminated by either you or Twitter as follows.
- You may end your legal agreement with Twitter at any time for any or no reason by deactivating your accounts and discontinuing your use of the Services. You do not need to specifically inform Twitter when you stop using the Services. If you stop using the Services without deactivating your accounts, your accounts may be deactivated due to prolonged inactivity under our Inactive Account Policy.
- We may suspend or terminate your accounts or cease providing you with all or part of the Services at any time for any or no reason, including, but not limited to, if we reasonably believe: (i) you have violated these Terms or the Twitter Rules, (ii) you create risk or possible legal exposure for us; or (iii) our provision of the Services to you is no longer commercially viable. We will make reasonable efforts to notify you by the email address associated with your account or the next time you attempt to access your account.
- In all such cases, the Terms shall terminate, including, without limitation, your license to use the Services, except that the following sections shall continue to apply: 4, 5, 7, 8, 10, 11, and 12.
- Nothing in this section shall affect Twitter's rights to change, limit or stop the provision of the Services without prior notice, as provided above in section 1.

11.Disclaimers and Limitations of Liability

- Please read this section carefully since it limits the liability of Twitter and its parents, subsidiaries, affiliates, related companies, officers, directors, employees, agents, representatives, partners, and licensors (collectively, the "Twitter Entities"). Each of the subsections below only applies up to the maximum extent permitted under applicable law. Some jurisdictions do not allow the disclaimer of implied warranties or the limitation of liability in contracts, and as a result the contents of this section may not apply to you. Nothing in this section is intended to limit any rights you may have which may not be lawfully limited.

A. The Services are Available "AS-IS"

- Your access to and use of the Services or any Content are at your own risk. You understand and agree that the Services are provided to you on an “AS IS” and “AS AVAILABLE” basis. Without limiting the foregoing, to the maximum extent permitted under applicable law, THE TWITTER ENTITIES DISCLAIM ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.
- The Twitter Entities make no warranty or representation and disclaim all responsibility and liability for: (i) the completeness, accuracy, availability, timeliness, security or reliability of the Services or any Content; (ii) any harm to your computer system, loss of data, or other harm that results from your access to or use of the Services or any Content; (iii) the deletion of, or the failure to store or to transmit, any Content and other communications maintained by the Services; and (iv) whether the Services will meet your requirements or be available on an uninterrupted, secure, or error-free basis. No advice or information, whether oral or written, obtained from the Twitter Entities or through the Services, will create any warranty or representation not expressly made herein.

B. Links

- The Services may contain links to third-party websites or resources. You acknowledge and agree that the Twitter Entities are not responsible or liable for: (i) the availability or accuracy of such websites or resources; or (ii) the content, products, or services on or available from such websites or resources. Links to such websites or resources do not imply any endorsement by the Twitter Entities of such websites or resources or the content, products, or services available from such websites or resources. You acknowledge sole responsibility for and assume all risk arising from your use of any such websites or resources.

C. Limitation of Liability

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE TWITTER ENTITIES SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, OR ANY LOSS OF PROFITS OR REVENUES, WHETHER INCURRED DIRECTLY OR INDIRECTLY, OR ANY LOSS OF DATA, USE, GOOD-WILL, OR OTHER INTANGIBLE LOSSES, RESULTING FROM (i) YOUR ACCESS TO OR USE OF OR INABILITY TO ACCESS OR USE THE SERVICES; (ii) ANY CONDUCT OR CONTENT OF ANY THIRD PARTY ON THE SERVICES, INCLUDING WITHOUT LIMITATION, ANY DEFAMATORY, OFFENSIVE OR ILLEGAL CONDUCT OF OTHER USERS OR THIRD PARTIES; (iii) ANY CONTENT OBTAINED FROM THE SERVICES; OR (iv) UNAUTHORISED ACCESS, USE OR ALTERATION OF YOUR TRANSMISSIONS OR CONTENT.
- IN NO EVENT SHALL THE AGGREGATE LIABILITY OF THE TWITTER ENTITIES EXCEED THE GREATER OF ONE HUNDRED U.S. DOLLARS (U.S. $100.00) OR THE AMOUNT YOU PAID TWITTER, IF ANY, IN THE PAST SIX MONTHS FOR THE SERVICES GIVING RISE TO THE CLAIM.
- THE LIMITATIONS OF THIS SUBSECTION SHALL APPLY TO ANY THEORY OF LIABILITY, WHETHER BASED ON WARRANTY, CONTRACT, STATUTE, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, AND WHETHER OR NOT THE TWITTER ENTITIES HAVE BEEN INFORMED OF THE POSSIBILITY OF ANY SUCH DAMAGE, AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

12. General Terms

A. Waiver and Severability

- The failure of Twitter to enforce any right or provision of these Terms will not be deemed a waiver of such right or provision. In the event that any provision of these Terms is held to be invalid or unenforceable, then that provision will be limited or eliminated to the minimum extent necessary, and the remaining provisions of these Terms will remain in full force and effect.

B. Controlling Law and Jurisdiction

- These Terms and any action related thereto will be governed by the laws of the State of California without regard to or application of its conflict of law provisions or your state or country of residence. All claims, legal proceedings or litigation arising in connection with the Services will be brought solely in the federal or state courts located in San Francisco County, California, United States, and you consent to the jurisdiction of and venue in such courts and waive any objection as to inconvenient forum.
- If you are a federal, state, or local government entity in the United States using the Services in your official capacity and legally unable to accept the controlling law, jurisdiction or venue clauses above, then those clauses do not apply to you. For such U.S. federal government entities, these Terms and any action related thereto will be governed by the laws of the United States of America (without reference to conflict of laws) and, in the absence of federal law and to the extent permitted under federal law, the laws of the State of California (excluding choice of law).

C. Entire Agreement

- These Terms, including the Twitter Rules for the Twitter Services, and our Privacy Policy are the entire and exclusive agreement between Twitter and you regarding the Services (excluding any services for which you have a separate agreement with Twitter that is explicitly in addition or in place of these Terms), and these Terms supersede and replace any prior agreements between Twitter and you regarding the Services. Other than members of the group of companies of which Twitter, Inc. is the parent, no other person or company will be third party beneficiaries to the Terms.
- We may revise these Terms from time to time, the most current version will always be at twitter.com/tos. If the revision, in our sole discretion, is material we will notify you via an @Twitter update or e-mail to the email associated with your account. By continuing to access or use the Services after those revisions become effective, you agree to be bound by the revised Terms.
- If you live in the United States, these Terms are an agreement between you and Twitter, Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103 U.S.A. If you live outside the United States, your agreement is with Twitter International Company, an Irish company with its registered office at The Academy, 42 Pearse Street, Dublin 2, Ireland. If you have any questions about these Terms, please contact us.
- Effective: May 18, 2015
  Archive of Previous Terms

Back to Social Media