Carshalton College Kingston College Merton College South Thames College

South Thames Colleges Group

ICT SECURITY POLICY
August 2019

SOUTH THAMES COLLEGES GROUP
KINGSTON HALL ROAD
KINGSTON
SURREY KT1 2AQ

Contents

1. Definitions

The term “ICT” refers to any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

The term “user” refers to any person who accesses an ICT system, service or equipment owned, managed or supplied by the College or one of its partners.

The term “visitor” refers to any person who accesses an ICT system, service or equipment owned, managed or supplied by the College or one of its partners, but is not a student or member of staff.

2. Audience

This document is for all users & providers of ICT equipment and services within the Colleges Group.

Acceptable Use Policy for ICT Users & Acceptable Use Policy for Email applies to all who use ICT equipment and services, within the Colleges Group.

Acceptable Use Policy for the Service Providers applies to all that provide ICT equipment and services to the user community in the Colleges Group.

Acceptable Use Policy for Mobile Devices applies to all users that carry out Colleges Group business on a Mobile Device be it their own personal or Organisation owned.

Acceptable Use Policy for the Use of Social Networking Sites applies to all Colleges Group Users who use Social Networking Sites.

3. Introduction

This ICT Security Policy forms a key part of the South Thames Colleges Group overall Information Security Policy. The ICT Security Policy focuses on the technical and usage issues in relation to the Colleges Group ICT systems whereas the Information Security Policy governs the broader issues of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so.

In using Information Communication Technology (ICT), users within the Federation have the ability to create, store and/or access a wide range of electronic information. The aim of the policy outlined in this document is to ensure that:

- The relevant information is always available to the relevant users.
- Confidentiality is always maintained.
- The integrity of the information is maintained.
- Data access and use conforms with regulations in regard to the General Data Protection Regulation 2018 & Data Protection Act 2018.

This policy is to enforce the appropriate use of ICT within the South Thames Colleges Group and is reinforced by recommendations from JISC & UKERNA in line with ISO27001. The UCISA Information Security Toolkit (March 2015), designed to encourage best practice, has also been used as a foundation for this document.

The College needs to be aware of ICT security as there is a range of undesirable consequences associated with breaches of ICT security which include but are not limited to:

- Systems being unavailable
- Bad publicity and embarrassment
- Fraud
- Illegal personal investigation
- Industrial espionage
- Terrorism

This Policy comprises the following sections:

1. **Definitions** – This section defines terms used within this policy document.

2. **Audience** – This section states the audience to which this document applies.

3. **Introduction** – This section provides an overview of the policy.

4. **Relevant laws and regulations** – Covering the underpinning legislative framework.

5. **Information Security Policy.**

6. **Data Protection Policy.**

7. **The Prevent duty** – Requirement from the Counter-Terrorism and Security Act 2015.

8. **Management** – This section covers the management responsibilities such as incident handling, reviewing this policy and communication of this policy to users.

The following policies, which support this document, have been included here as appendices:

Appendix A: Acceptable Use Policy (AUP) for ICT users – This section sets out the framework for governing use of ICT systems and services by individuals of South Thames Colleges Group. This is the primary document that most users will need to read and accept.

Appendix B: Acceptable Use Policy for ICT service providers – This section sets out the security framework for the provision of Information Services that go beyond AUP for ICT users section, in that it involves service provision rather than solely Information Services. This policy has a major impact on IT Services as the main provider of services but also impacts anyone providing services for others, e.g. College; Schools; LRC.

Appendix C: Acceptable Use Policy for Email – This section sets out the framework for governing the use of the South Thames Colleges Group Email systems.

Appendix D: Acceptable Use Policy for Mobile Devices – This section sets out the security framework for using mobile devices for Colleges Group business.

Appendix E: Acceptable Use Policy for the Use of Social Networking Sites – This section sets of the framework governing the use of social Networking.

4. Relevant Laws and regulations relating to this document

It is the policy of the South Thames Colleges Group that all of its activities must be conducted in accordance with current legislation. If a user of information is unsure as to their responsibilities in relation to the laws they should seek advice through their immediate supervisor.

The use of information is governed by a variety of different Acts of Parliament. These currently include but are not fully exclusive of:
The Copyright, Designs and Patents Act 1988
The Data Protection Act 1998
The Human Rights Act 1998
The Computer Misuse Act 1990
The Regulation of Investigatory Powers Act 2000
The Freedom of Information Act 2000
The Electronic Communications Act 2000
The Digital Economy Act 2010
The Counter-Terrorism and Security Act 2015
The General Data Protection Regulation – 2018
The Data Protection Act 2018

Together with various Statutory Instruments, and other pieces of legislation.

In regards to dealing with breaches of this policy that are not criminal the appropriate College or partner organisation polices will be referred to.

5. Information Security Policy

The College 'Information Security Policy' is to be read in conjunction with the ICT Security Policy.

6. Data Protection Policy

The Groups 'General Data Protection Policy' is to be read in conjunction with the ICT Security Policy.

7. The Prevent duty

This statutory guidance makes clear the need for Colleges to ensure that Staff and Students are safe from terrorist and extremist material when using ICT Equipment (this includes Smart Phones & Tablets), while accessing College supplied services such as access to the internet.

Therefore in addition to the Filtering Systems that IT Services have in place, the Colleges Group has clear policies for Staff and Students in the use of ICT on College premises in relation to research of Terrorism and Counter Terrorism as part of the Learning and Teaching.

These Policies are separate to the ICT Policies covered in this document.

8. Management Issues

In order for this policy to be employed effectively it is essential that those in a managerial position are personally fully aware of it and apply it in their own use of ICT.

Managers are responsible for:

- Ensuring that their staff, students and visitors only use ICT when they have agreed to follow the policy. This includes staff working in Collaborative Partner institutions who have access to College systems.

- For handling any disciplinary issues that arise and proactively investigating any suspected breaches.

- Enforcing the requirements of the ‘Prevent’ Agenda, in relation to the use of ICT in the research of Terrorism and Counter Terrorism by Staff and Students as part of the Learning and Teaching.

Students will be notified of the policy when they enrol. Staff will be notified of the policy when they sign their contract of employment, or in the case of Collaborative Partners, when they complete the Data Collection template.

Visitors to the College will only be granted access to College systems once they have signed to accept the policy.

The policy and any changes will be made available through the Intranet and VLE. Paper copies of the policy will also be available from the LRC.

Acceptance of this Policy
All existing users of ICT will be notified of this policy and future changes. The users continued use of ICT after notification will constitute acceptance and agreement to the policy document.

Disciplinary Action
Breaches of any sections of this policy are potentially disciplinary issues which will be handled by existing staff or student disciplinary procedures. Staff and Students must comply with the policy. Failure to do so may render them liable to disciplinary action which could, in serious cases, lead to dismissal from their employment or course.

Security Breaches
Any suspicion of breach of the policy must be reported to the central Helpline immediately. Failure to do so constitutes a breach of this policy. There may be some instances e.g. sensitivities, where users then may report a suspected breach to their line manager. The line manager then must report the issue to the central Helpline or direct to the Director of IT Services.

Within the current Colleges Group guidelines the Head of Infrastructure has the power to authorise IT Services staff to suspend access to all accounts affected by the breach. The Head of Infrastructure has the authority to suspend these accounts as well. Suspensions will be lifted in three working days unless further suspension is authorised by the Director of IT Services.

In cases where investigation of traffic or content of user accounts is necessary then IT Services staff will carry out such work under direct instruction from the Head of Infrastructure following authorisation from the Director of IT Services or Director of HR (Staff) or Principal/Vice Principal (Students). South Thames Colleges Group will involve the Police in all cases where they believe illegal activity may have taken place.

Updates and Amendments
IT Services will ensure this policy is reviewed annually to reflect best practice with revisions being approved by the GLT.

This policy document will be updated and amended as required.

This document has been approved by the following:

Group / Person	**Date Approved**
Director of IT Services	
GLT	

APPENDIX A

1 Acceptable Use Policy for ICT Users

This AUP forms part of the South Thames Colleges Group regulations. The Colleges Group is committed to maintaining standards. All users of ICT facilities must conform to Health and Safety requirements. The Colleges Group reserves the right to investigate computer activity that is suspected to be detrimental to any persons, service or network or to be in breach of the AUP herein.

2 Scope

This policy applies to users of all central and departmental ICT facilities (including software) owned, leased or hired by the South Thames Colleges Group, all users of ICT facilities on College premises and all users of any ICT facilities connected to the Organisation networks.

3 The Legal Framework

Use of the ICT facilities is subject (inter alia) to the provisions of the following Acts:

- Data Protection Act 1998
- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Digital Economy Act 2010
- Human Rights Act 1998
- Counter-Terrorism and Security Act 2015
- And any regulations made pursuant to these Acts.

Offences might be reported to the Police for further investigation and possible prosecution. Full details of the legislation are available on the Internet.

4 Authorisation

Use of any ICT facility is open only to staff, Colleges Group Partners and enrolled students of South Thames Colleges Group and any other persons authorised by the Manager of the facility (e.g. including visiting lecturers).

5 Registration

Use of the facilities is conditional upon prior registration and the granting of a Username and an individual password. Such registration is carried out by HR/Student Services.

6 Access

On-Site ICT facilities will be accessible during published opening hours, or in certain circumstances by special arrangements. Remote access to some facilities is available 24/7 with best endeavours. Access will be contingent on system maintenance requirements.

7 Conditions of use for Hardware and Software

Users must not in any way cause any form of damage to the College computing equipment or software, nor to any of the rooms and their facilities and services which contain that equipment or software; nor to any of the network wiring infrastructure or communications equipment. The term "damage" includes modifications to hardware, software or infrastructure which, whether or not causing harm to the hardware or software, incur time and/or cost in restoring the system to its original state. All costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements will be charged to the person or persons causing the damage. The costs will be determined by IT Services.

Users must comply with the terms and conditions of all licence agreements, available from the Managers of the ICT facilities, relating to any part of those facilities including software, equipment, services, documentation or other goods.

Users must not modify any software, nor incorporate parts of any software into their own work, without written permission from the copyright/intellectual property owner and the Manager of the ICT facility.

Users must comply with any instructions or regulations displayed in and around computing facilities.

Users must not introduce any virus, worm, malware, trojan horse or any other "nuisance" program or file onto any system or take any action to circumvent or modify any precautions taken by the College to prevent "infection" of its machines.

Users must not use the ICT facilities for sending any message textual or graphic or voice or video that is offensive, abusive, obscene, defamatory, racist, terrorism related or otherwise unlawful. Users must not initiate or spread electronic chain mail. Any electronic mail must be relevant to the user's course of study or job within the Colleges Group and it must be sent only to those users to whom it is relevant.

Users may only access their own files and files which they have been given express permission to access.

Users must not use another user's Username or permit or allow another user to use his/her own Username.

Users must not allow any password associated with his/her Username to become known to another user. The user will be held responsible for any unlawful action carried out under his/her computer account unless there is evidence to prove otherwise.

Users must not make known any other passwords which may be supplied to them in order to enable access to subscribed electronic resources.

Users must not connect any equipment to the College wired network without prior authority from IT Services Head of Infrastructure.

Every user of network facilities shall comply with any rules published for use of the networks and/or any ICT systems to which he/she has access over those networks.

Users must terminate each session in accordance with published instructions.

Interference with or removal of printout which belongs to another person is not permitted. Uncollected printout will be disposed of.

Printing credit in a student account will not be refunded at any time during the year or at the end of the academic year. Continuing students will carry their paid for printing credit to the following year. Students leaving the College will not be refunded.

8 Behaviour

The creation, display, production, downloading, uploading and circulation of offensive and/or terrorist related material in any form or on any medium is forbidden.

Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using facilities.

No equipment should be moved from its designated place or be tampered with in any way.

9 Equipment Loans

No equipment or software may be borrowed without permission from the Manager of the ICT facility where available.

Security are authorised to stop and question any person seen leaving College premises with ICT equipment or software.

10 Private and Commercial Use

The use of any of the College’s ICT facilities for commercial gain as well as for private work (unconnected with a student's course or study at the College or a member of staff's legitimate activities) or for work on behalf of others is not allowed unless prior agreement has been made with the Manager of the ICT facility in question and an appropriate charge for that use has been determined.

11 Use of JANET and the Internet

Use must comply with the JANET Acceptable Use Policy (available from https://community.jisc.ac.uk/library/acceptable-use-policy), as published by the United Kingdom Education and Research Networking Association (UKERNA), which states that:

Subject to the following paragraphs, JANET may be used for any legal activity that is in furtherance of the aims and policies of the College.

The following constitutes Unacceptable Use of JANET

JANET may NOT be used for any of the following (8 to 16.7 inclusive):

8. Janet may not be used by a User Organisation or its Members for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities.

9. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

10. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.

11. Creation or transmission of material with the intent to defraud.

12. Creation or transmission of defamatory material.

13. Creation or transmission of material such that this infringes the copyright of another person.

14. Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.

15. Deliberate unauthorised access to networked facilities or services.

16. Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:

16.1 wasting staff effort or Janet resources, including time on end systems on another User Organisation's network, and the effort of staff involved in the support of those systems;

16.2 corrupting or destroying other users' data;

16.3 violating the privacy of other users;

16.4 disrupting the work of other users;

16.5 denying service to other users (for example, by overloading of access links or switching equipment, of Janet services, or of services or end systems on another User Organisation's network);

16.6 continuing to use an item of software or hardware after the Janet Network Operations Centre or its authorised representative has requested that use cease because it is causing disruption to the correct functioning of Janet;

16.7 other misuse of Janet, such as the introduction of "viruses" or other harmful software via Janet to resources on Janet, or on another User Organisation's network.

Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET.

12 College Rules for using Janet and the Internet

Commercial use is prohibited. Commercial use refers to any activity connected or involving any trade, profession, vocation or business not being any part of any function or purpose of the South Thames Colleges Group whether carried on solely or jointly or severally and/or whether or not with a view to profit or benefit any person or personal body other than the South Thames Colleges Group and its Partners.

Recreational student use is allowed but students have to release the workstations if needed for course-related work. Unreasonable or recreational use by staff is prohibited during working hours.

Anonymous Email or any type of anonymous electronic information must not be sent.

Offensive material must not be sought or knowingly received.

The JANET Acceptable Use Policy applies also to the internal College network.

Network services (e.g. Ftp or Web servers) must not be set up without first being registered with IT Services. The person setting up the service will be held responsible for the secure operation of that service.

The College's Information Security Policies should be read as part of the Colleges Group regulations.

13 Disclaimers

South Thames Colleges Group accepts no responsibility for the malfunctioning of any equipment or software that results in the failure of security or integrity of any stored program or data.

Student files and access will be removed once the student is no longer on his/her course. Students are advised to make copies on removable media of any data that they store on College services if they wish to keep it beyond this time, as the College will not be liable for its non-retention.

Staff computer account will be disabled once the member of staff's contract has been terminated, and deleted after 30 days. The College will not be liable for the non-retention of the member of staff's files beyond this time.

14 Monitoring & Access of ICT Systems & User Accounts

The South Thames Colleges Group may at any time permit the inspection, monitoring, or disclosure of ICT Systems and Data.

- **When required by and consistent with English law**

The South Thames Colleges Group evaluates all such requests against the precise provisions of the Freedom of Information Act, General Data Protection Regulation, The Data Protection Act, The Regulation of Investigatory Powers Act, and other laws concerning disclosure and privacy, or other applicable law.

- **Policy compliance**

At the written request of the Principal, Vice-Principal, Director of IT Services or Director of HR, if there are reasonable grounds to believe that violations of Colleges Group policies have taken place.

The College reserves the right to monitor ICT Systems:

- For instance to carry out system management, problem resolution, maintenance and capacity planning, to correct problems or for similar reasons related to performance or availability of the system.

- To address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system.

- The College may access, with the written request of the Principal, Vice-Principal, Director of IT Services or Director of HR, the content of user accounts.

- To meet time-dependent, critical business or operational needs or to carry out records management responsibilities; e.g. to conduct business during a crisis if an employee is absent when information is required, or prolonged absence of an employee when information in the User's account is required. The User will generally be informed at the earliest opportunity if this form of access is necessary.

15 Disciplinary Procedures

Failure to comply with these conditions of use for facilities may result in the following procedures being invoked:

- Withdrawal (whether permanent or temporary) of access to College ICT facilities. Such withdrawal may be invoked immediately after suspected breach of ICT regulation(s) has occurred. Reinstatement of access to ICT facilities will be through normal disciplinary procedures.
- Recommendation to proceed through the Colleges Group disciplinary processes including exclusion from the College (student) or termination of contract (staff).
- Referral to the Police for possible prosecution. Where appropriate.

THE DATA PROTECTION ACT (2018) applies to all users of the College's computers who process personal data (information relating to a living person). Further information and guidance regarding the requirements of the Act may be obtained from the Colleges Group Data Protection Officer, or from the website of the Information Commissioner's Office: http://www.ico.org.uk

APPENDIX B

Acceptable Use Policy for the Service Providers

1 Scope of this Policy

This policy applies to any ICT equipment and services that are accessed by South Thames Colleges Group users. This includes servers (data, web, application, others), information on servers, and communications equipment. Within this document all such devices are referred to as "systems". Most of these systems are operated by IT Services staff but this policy also applies to any member of the South Thames Colleges Group operating such equipment, for example a web server on an externally hosted platform.

The "Acceptable Use Policy for ICT Users" also applies to staff involved in an ICT provider role.

2 Roles

Within this policy a number of roles are referred to as defined below:

Service Owner – these are staff with the final authority for any item of equipment, software or set of information. For example the Director of HR would be the owner of HR system.

Process Owner – these staff are responsible for the business process that the ICT service supports. For example the payroll process would be owned by the HR Payroll Manager.

Service Managers – these are staff who have been delegated by the service owner to carry out system management functions. Members of IT Services often carry out this role on behalf of service owners.

Head of Infrastructure – this member of staff has responsibility for ensuring that this policy is enforced.

Infrastructure Team – these staff carry out work that involves changing ICT systems. They have a duty to ensure that work carried out complies with this policy. If appropriate they will implement automated security measures.

Senior Support Technician – this member of staff is responsible for the day to day running of the individual College ICT operations, including managing the operational staff and environment.

Operational Staff – these staff carry out work to ensure the correct operation of ICT systems in accordance with this policy.

User Managers – these are managers of end users, normally Heads of Schools, Heads of Service and Corporate Departments and Support Directors, who have a key role in approving requests for their staff to be granted access to information systems.

3 Registration of ICT Systems

All systems that fall within the scope of this policy must be registered with the Head of Infrastructure and operated as agreed.

4 Secure Network Boundaries

Security Zones – the network will be designed to create security zones to reduce the possibility of internal or external users gaining unauthorised access to systems. ICT systems with particularly high security vulnerabilities will be protected both from internal and external access. All other systems by default will be protected from external access.

Remote Access Facilities – all users can gain access to a number of the IT Systems externally via their own internet service providers thus connecting to the College through its main firewalled external pipe.

Remote Management Facilities – in special cases where it is necessary for users to connect directly into the College externally e.g. Operational staff out of hours maintenance, this will only be allowed with the service owners' approval, and only once security measures have been taken to ensure a secure connection.

5 Management of the Production Systems Environment

The logical; and physical operational environment requires particular thought as access to this environment normally circumvents conventional ICT security. User ID's & passwords used in this environment that provide privileged access to systems for system management and operational reasons must be managed as below.

Privileged Account ID's – these user ID's will normally be allocated to specific staff but will **NOT** be the same as the ID they used for their daily access. In some cases these privileged accounts are dictated by the system hence are used by more than one member of staff but this will be avoided wherever possible.

Privileged Account Creation/Modification – accounts will only be created with the written authority of the Service owner or his/her deputy, in conjunction with the Infrastructure Manager.

Access rights – account configuration will be carefully considered to allow access only to appropriate information on the system as agreed by the Service owner. If necessary a member of staff may be issued multiple user ID's so that the privileged ID is only used when desired by their role.

Account Deletion – privileged accounts will be removed immediately they are not required for either operational or staffing reasons.

Passwords – all the principles defined for the management of passwords apply. Whenever system admin passwords are changed copies must be logged with the Head of Infrastructure and Service Owner.

External Staff – access to live systems by external support staff must be supervised by ITS operational staff and only once agreed by the Director of IT Services or Head of Infrastructure.

Physical Environment – access to systems and system consoles can allow normal security measures to be circumvented. All environments where such equipment is located must be physically secure and access limited as defined by procedures.

6 Backup and Media Control

All systems must be backed up to removable media and copies stored in a secure remote location, if the solution is site based. This control does not apply to an Off-Site (Hosted) Backup Solution.

Backup Media Storage – the media must be stored in fire proof safe remote from the physical system that has been backed up.

Backup Frequency – all data must be regularly backed up.

Fault Tolerant Equipment – critical information systems where 24/7 service is required; consideration must be given to deploying fault tolerant equipment such as redundant power supplies and Redundant Storage configurations.

7 Computer Viruses and Similar

Definitive measures must be in place to protect against the introduction, spread or storage of such programmes. Some can be quite harmful, erasing data or causing your hard disk to require reformatting. A virus that replicates itself by resending itself as an e-mail attachment or as part of a network message is known as Malware. All ICT systems must be running adequate anti virus protection as defined.

8 Managing User Accounts

The following must be followed in relation to the management of user accounts on all ICT equipment:

User IDs – where a service is provided to more than one department the standard College ID should be used as issued by IT Services.

Account Creation/Modification – accounts will only be created within the guidelines agreed by the service owner.

Staff the account holder must have a valid HR issued ID number.

Students the account holder must have a valid student ID number issued by Student Administration.

Access Rights – all accounts will be configured to allow access only to information on the system as defined by the service owner in accordance with the users' role.

Account Deletion – procedures must be in place to remove accounts when no longer required.

Staff - the account will be disabled immediately the staff member leaves the South Thames Colleges Group, on notification by HR. Full deletion will follow in 30 Days.

Student - accounts will be disabled when they are no longer shown as current via EBS data feed. The accounts will be deleted 90 days later, unless they are a returning student.

Account Suspension – procedures must be in place to suspend accounts instantly upon request from either the Director of IT, the Human Resources Director, the Director of Student Services and External Relations or the Vice Principal.

Staff – the account will be suspended immediately the staff member breaches the ICT Security & Usage Policy, or for other reasons (such as long term sick leave) on direct notification from the Human Resources Director.

Student accounts will be suspended immediately the student breaches the ICT Security & Usage Policy, or for other reasons on direct notification from the Principal or Vice-Principal.

9 Managing Shared Accounts

Shared accounts are only allowed for special purposes on the written approval of the Head of Infrastructure when their functionality is suitably restricted. These accounts will instantly be disabled when deemed necessary by the Head of Infrastructure in conjunction with the service owner.

10 Anonymous and Guest Accounts

All accounts must be password protected and be associated to at least one named user who takes responsibility for additional accounts. Thus anonymous and guest accounts must not exist on any system.

11 Managing User Passwords

All accounts must have passwords, and they must be created adhering to the following principles.

Structure of Passwords – passwords will be at least 8 characters long, and should be alphanumeric and contain at least one other character of another type. Their structure must be random and meet password complexity requirements. Recognisable passwords may be allowed where the user is forced to change it the first time they log in. The new password must follow the structure as stated.

Initial Passwords – all accounts are allocated a random password on creation. Registered students, based at College, will receive these passwords when they first log into a College machine; students from external institutions will need to obtain their password via a recognised proxy. Passwords for new staff will be sent to their line manager in time for their first day.

Password Changing by Users – all users have access to a secure system to change their own passwords. It is the responsibility of the user to change their password as required by their own risk analysis of the type and age of their chosen password.

Password Changing by System Support Staff – only the owner of the account can ask for their account password to be reset. This usually occurs if they forget their password. IT Services staff will change the password once ID has been verified. The user will be prompted to change the password on their first login with the new password.

Not displayed – passwords should never be displayed on screens or on physical media such as paper or post-it notes.

Inactivity – staff must lock their desktops or log out if they are leaving their machine unattended. Students must not leave a desktop unattended, they must log out.

Incorrectly Entered Passwords – all unsuccessful logins will be logged. After 5 incorrect attempts within a period of 10mins the account will be locked and will automatically reset after 10 Minutes.

12 Data Protection Act

All data relating to individuals must be stored in securely and managed and processed in accordance with the Data Protection Act. Details relating to the Data Protection Act 2018 may be obtained from the Colleges Group Data Protection Officer.

13 Investigating Security Incidents

At times it will be necessary for IT Services staff when authorised by the Principal, Vice-Principal, Director of IT Services or Human Resources Director, to carry out investigations on suspected security incidents and other situations.

APPENDIX C

Acceptable Use Policy for Email

1 Scope of this Policy

This policy applies to all users of the College Email system. Email is available to all users within the Colleges Group community who have agreed to abide by the Acceptable Use Policy for ICT Users.

2 Responsible Use of Email

Users sending Email from any South Thames Colleges Group owned domain, are seen as representatives of the Group and as such should act in a responsible manner.

The sending of abusive, offensive, defamatory, racial, terrorist related or sexual content within an Email is strictly prohibited.

The sending of Email that could be considered libellous to an individual or organisation is strictly prohibited.

3 Personal Use of Email

Users are permitted to use the Email systems for personal use providing they adhere to the following:

- Personal views are clearly stated as such.
- Purpose is not for financial gain to the user or other organisation.
- The use does not contravene Acceptable Use Policy for ICT users.
- All personal email must be stored in a folder clearly marked as personal.

4 Email Security

Email is not a secure form of communication and as such users must realise that any information sent via Email may be seen by other persons. Users are responsible for ensuring they don't compromise Information Security.

- The confidentiality of Email cannot be assured and as such users should carry out a risk assessment before sending confidential or sensitive information via Email.
- Users must not intercept or access other users Email without proper grounds and authorisation, and in accordance with the law.

5 Monitoring and Access to Email

The Colleges Group may at any time permit the inspection, monitoring, or disclosure of Email content;

When required by and consistent in law

The South Thames Colleges Group does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Freedom of Information Act, Data Protection Act, The Regulation of Investigatory Powers Act, and other laws concerning disclosure and privacy, or other applicable law.

Policy compliance
At the written request of the Director of IT Services or HR Director (Staff) or Principal/Vice-Principal (Students), if there are reasonable grounds to believe that violations of College policies have taken place.

The College reserves the right to monitor Email in order:

- To carry out system management, problem resolution, maintenance and capacity planning, to correct addressing problems or for similar reasons related to performance or availability of the system

- To address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system

- The Colleges Group may access, with written authorisation by the Principal, Vice-Principal; the HR Director or Director of IT Services, the content of any Email held on the Colleges Group System.

- To meet time-dependent, critical business or operational needs or to carry out records management responsibilities; e.g. to conduct business during; a crisis if an employee is absent when information is required a prolonged absence of an employee when information in the User's Email is required. The User will generally be informed at the earliest opportunity if this form of access is necessary.

6 SPAM

SPAM is defined as bulk Email communications that are unsolicited and not authorised by the Colleges Group GLT. For example an invitation to a personal birthday party sent to the entire user community would be considered SPAM.

- Users are strictly prohibited from the sending of SPAM within any of the Colleges Group domains.
- Users are also strictly prohibited from sending SPAM from a Colleges Group domain to any other domain worldwide.

7 Attachments

Network bandwidth is a valuable commodity to the College and as such users must be responsible when sending Email attachments.

Attachment limits for Email have been set at 25MB. This is a restriction not a target.

Users must not send harmful or dangerous content as Email attachments such as virus or worms. The sending and forwarding of chain emails is also prohibited.

The sending of multimedia content such as video or music files must be considered carefully, as this can have a serious impact on network bandwidth & storage.

8 Malware

Malware is a term used to describe a broad category of damaging software that includes viruses, worms, trojan horses, rootkits, spyware, adware. The effects of malware range from brief annoyance to computer crashes, identity theft and inability to access your data. Avoiding malware involves a two-part strategy.

- **From a website:** If you are unsure, leave the site and research the software you are being requested to install. If it is OK, you can always come back to the site and install it.
- **From e-mail:** Do not trust anything associated with an e-mail from people you do not know, especially when the message contains links or attachments.

APPENDIX D

Acceptable Use Policy for Mobile Devices

1 **Scope of this Policy**
This policy applies to all users of mobile devices that are used for South Thames Colleges Group business. If the Mobile device is owned by the Colleges Group the user must agree to this policy or return the portable to their line manager.

2 **Types of Mobile Device Available**
Examples of the mobile devices the College supplies to its users, as authorised by their line manager are:

- Laptops
- Mobile Phones
- PDAs
- Tablets

Colleges Group supplied devices are authorised to be connected to the College ICT Infrastructure. Mobile device users must comply with all applicable Acceptable User Polices as defined in the ICT Security Policy.

3 **Personal Use of Colleges Group owned Mobile Devices**
Users are permitted to use Organisation owned Mobile Devices for personal use providing they adhere to the following:

- Any personal calls or data use are clearly declared to managers, at which point a charge maybe incurred.
- The purpose or use is not for financial or any other form of commercial gain to the user or other organisation.
- The use does not contravene the Acceptable Use Policy for ICT users.

4 **Physical Security of Colleges Group owned Mobile Devices**
Mobile devices if left unattended should be secured. For the working environment IT Services will make available desk locking cables for mobile device users where appropriate.

5 **Personal Use of Personal owned Mobile Devices**
Users are permitted to use Personally owned Mobile Devices to send/receive and store Colleges Group emails providing they accept the following:

- A Security Pin No. will be enforced onto your device to secure the unit, which will be required to be entered each time the device is used. After a set number of incorrect login attempts your Personal Device will be locked, and will require IT Services to reset.
- Built in Hardware encryption will be enabled to store Colleges Group emails. Older Mobile devices that do not support this feature will not be able to receive Colleges Group emails.
- Loss/Theft of your Personal Device must be immediately reported to IT Services so that Colleges Group Data can be remotely wiped from the device.
- The Personal use does not contravene the Acceptable Use Policy for ICT users.

6 **Room Storage –** Do not leave mobile devices unattended in open rooms. When the device is not in use it must be stored securely out of sight.

7 **Vehicle Storage –** Do not leave mobile devices in vehicles. However, if no alternative is available store in a locked boot out of sight. Vehicle storage must not be used over night or for long periods of time.

8 Data Security

Any Colleges Group data that is stored locally on a mobile device must be encrypted using the procedures set out by IT Services. Users must log into the mobile device to use it. All devices must have up to date Anti-Virus software installed (where available).

South Thames Colleges Group data must **not** be stored on any personal mobile devices that has not been secured as per point 5.

9 Device Abuse

Mobile device users must comply with The Acceptable User Policy for ICT Users.

APPENDIX E

Acceptable Use Policy for Use of Social Networking Sites

1 Scope of this policy

The policy applies to all Social Networking site users who have a relationship with the South Thames Colleges Group, either as a member of Staff or Partner, or as a Student. Social Networking sites include but are not limited to LinkedIn, Facebook, Myspace, YouTube and Twitter.

2 Responsible use of Social Networking

The Colleges Group understands the popularity and benefits of Social Networking sites if used responsibly. Such sites allow for, and promote, general communication, online discussion and provide the ability to share information about yourself and others quickly and easily. In many respects this can be beneficial to students and staff both in personal and academic terms. By following a few simple guidelines Social Networking can be enjoyed by all, safely and productively.

3 Guidelines for use of Social Networking

Before signing up to any Social Networking site make sure you have read the terms and conditions for that site, along with their privacy policy. If there is anything you do not understand or are not happy with, do **not** sign up to the site. When signing up to a site use only your personal details and not anyone else's. When filling in your personal details remember that these will be visible to other users. Only enter the details that you are happy with being in the public domain. It is **not** recommended that you fill in local addresses, telephone numbers or full dates of birth.

If you upload any pictures to your profile, license to use these pictures in many cases is transferred to the Social Networking site in question. This allows the site to use the photo how they want to, possibly in marketing and advertising.

You must **not** post any statements or photos that could damage the reputation of you, your family or that of the South Thames Colleges Group and its Partners. You must **not** make offensive or derogatory remarks about students, members of staff or other individuals, and you must **not** post obscene or derogatory images.

It is important to remember anything you post on Social Networking sites may be visible to anyone, anywhere, at anytime! It is important to be aware of the risks and take steps to protect yourself and your personal information. Posting personal information could potentially lead to unwanted attention and could even contribute to identity fraud. For your own benefit, you should not post details which you might find awkward later, for example something you would not want family members or a future employer to see.

It is important not to use the same username and password you use for other systems, such as your College login.

4 Monitoring

Social Networking Site Administrators, IT Services, Police and other agencies can and do monitor these sites from time to time. Users of these sites must keep in mind that they could face disciplinary action by breaching Colleges Group policies. They could also be subject to criminal proceedings if their actions are found to be illegal.

NOTE

It is now common practice for employers to search Social Networking sites as a means for screening potential applicants for positions of employment.