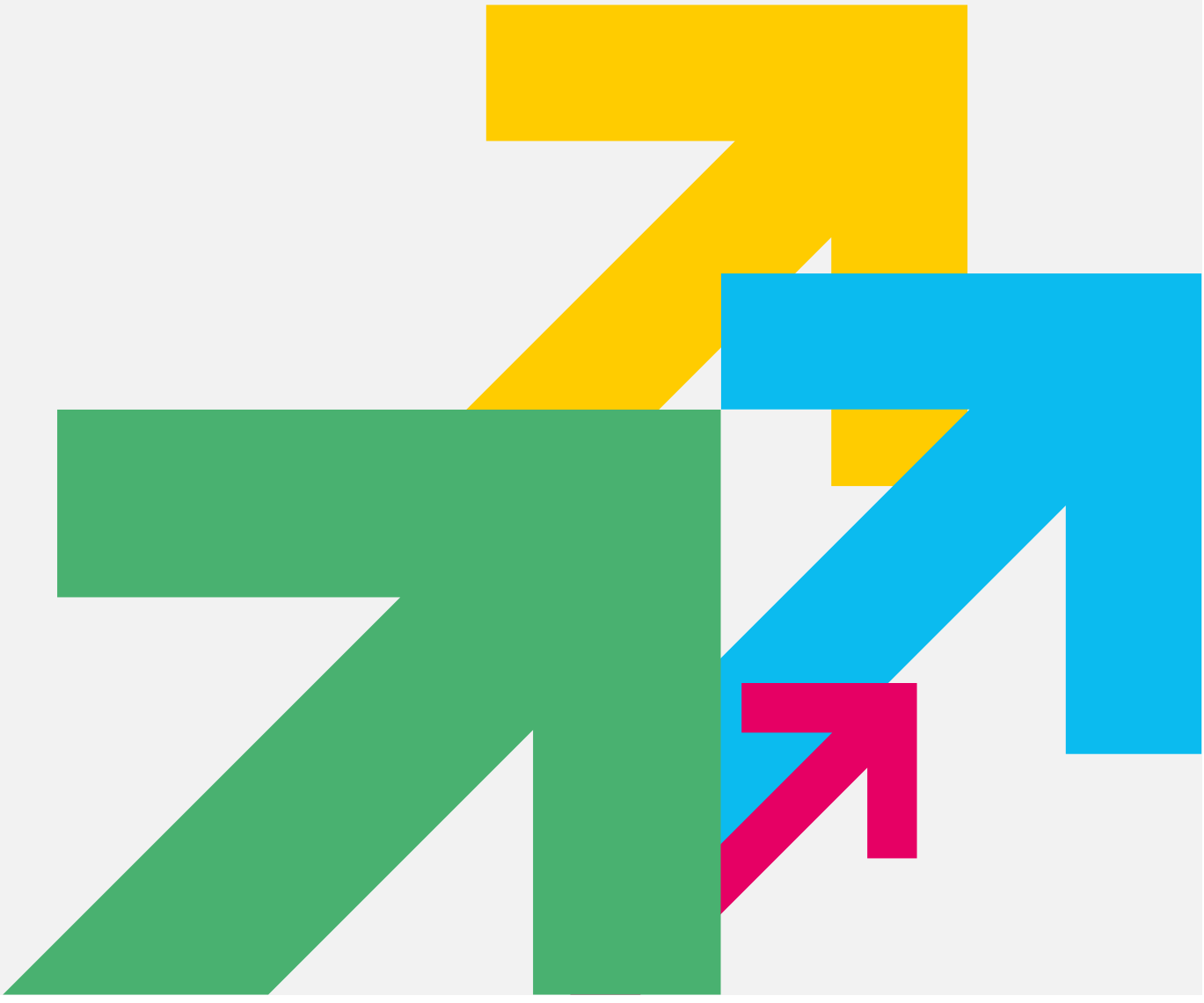
South Thames Colleges Group

Information Security Framework

July 2024

RAD Volo



Introduction

This document sets set out a framework for Information Security Management across the South Thames College Group. This incorporates all policies and procedures that are required to protect College Group information by maintaining;

- **Confidentiality:** protecting information from unauthorised access and disclosure.
- **Integrity:** safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion.
- **Availability**: ensuring that information and associated services are available to authorised users whenever andwherever required.
- **Resilience** of processing systems and services: the ability todefend against and mitigate the impact of a physical or technical incident and restore the availability and access to information in a timely manner.

Purpose

South Thames Colleges Group relies on the effective management and flow of information to enable staff to communicate and work effectively. The need to access information must be balanced with appropriate and proportionate measures to avoid the loss or unauthorised disclosure of confidential information.

The purpose of this policy is to establish an effective Information Security Management process to;

- Ensure our business continuity
- Protect our intellectual property rights, financial interests and completive edge
- Safeguard the interests and privacy of our students, staff andstakeholders and retain their trust
- Comply with the law and defend ourselves against legal action
- Maintain our reputation

Objectives

This framework sets set out the Groups Senior Management commitment to Information Security and establishes a framework of governance, responsibility and accountability for Information Security Management across the Group. The policies listed in this Framework applies to all information created or received in the course of Group business.

All members of the College Group have a responsibility to protect all confidential information to which they may have access in the course of their work.

Any user who breaches this framework may be liable to disciplinary action and may also be breaking criminal or civil law. Breaches of the policy which place the College Group at serious financial, commercial or reputational risk or actual loss may be considered as gross misconduct offences, for which dismissal may be an outcome.

Scope

The framework applies to all users of Group information. Users include all employees and students of the College Group, all contractors, suppliers, governors, College Group partners, and visitors who may have access to College Group information.

Policies/Documents relating to this Framework

IT Use Policy
This policy applies to all users of STCG IT facilities (including software) owned, leased or hired by the South Thames Colleges Group, and made available both on college premises and remotely connected to the Organisation networks. All Users must be familiar with this policy without exception.

IT Vulnerability Management Policy
This policy is a set of processes and procedures to identify and document STCG's approach to IT Vulnerability Management, including Patch Management.

IT Incident Management Policy
This policy is a process that aims to rapidly restore services to normal following an incident while minimizing adverse effects on the business.

IT Identity and Access Management Policy
This policy defines the process for the onboarding and off boarding of Staff and Student Accounts.

Information Security Policy
This policy applies to all users of STCG IT facilities (including software) owned, leased or hired by the South Thames Colleges Group, and made available both on College premises and remotely connected to the Organisation networks. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance; which could otherwise occur.

Cyber Security Policy
The policy applies to all students and staff and all members of the Colleges Group who have access to the Group IT systems and devices, both on the premises and remotely.

e-Safety Policy
The policy applies to all students and staff and all members of the Colleges Group who have access to the Group IT systems, both on the premises and remotely. This e-Safety Policy applies in all use of the internet and forms of electronic communication such as email, mobile phones, social media, instant messaging etc.

ICT Change Management Policy
This policy applies to all System Administrators who by the nature of their role will have privileged access to manage a system and are responsible for either authorising or carrying out maintenance work such as configuration changes, software upgrades and patches on STCG systems either run internally of supplied by a 3rd Party. This Policy outlines a process to be followed to make sure changes are completed with minimal disruption to our users.

IT Systems Password Policy
This policy applies only to System Administrators who by the nature of their role will have privileged access to manage a system and are responsible for the upkeep, configuration, change and reliable operation of that Computer systems either run internally of supplied by a 3rd Party to STCG. The Policy is to establish a standard for the creation of very strong passwords, the protection of those passwords, and the frequency of change of the passwords for System Administrator and other privileged accounts.

IT Asset Management Policy
This policy covers the lifecycle management and responsibilities of IT Assets within the STCG Group.

PC Build Standards
This document defines the minimum build and security standard for PC Desktop software provision across the Group.

Lines of Responsibility

All users of College Group information are responsible for

- Undertaking relevant training and awareness activities provided by the College Group to support compliance with this policy
- Taking all necessary steps to ensure that no breaches of information security result from their actions.
- Reporting all suspected information security breaches or incidents promptly so that appropriate action can be taken to minimise harm.