South Thames Colleges Group

Information Security Policy

July 2023

RAD Volo

INFORMATION SECURITY POLICY

Purpose

Information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as the South Thames College Group, where information will relate to learning, teaching, administration and management.

This policy is concerned with the management and security of College Group information assets. (An information asset is defined to be an item or body of information; an information storage system or an information processing system, which is of value to the organisation). The use made of these information assets by its members and others who may legitimately process College Group information on behalf of the College Group.

Scope

The Information Security Policy applies to all information which the College Group processes, irrespective of ownership or form.

Information Security Principles

- Information will be protected in line with all relevant College Group policies and legislation, notably those relating to data protection, human rights and freedom of information.
- Information will be made available solely to those who have a legitimate need for access.
- All information will be classified according to an appropriate level of security.
- The integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.

Legislation relevant to Information Security Policy

Data Protection Act 2018

Freedom of Information Act 2000

Privacy and Electronic Communications Regulations 2003

Regulation of Investigatory Powers Act (RIPA) 2000

Copyright, Designs and Patents Act 1988

Computer Misuse Act 1990

Counter-Terrorism and Security Act 2015

Records Management

The Group is required to retain certain information, whether held in hard copy or electronically, for legally defined periods. Such information must be appropriately safeguarded and not destroyed prior to the defined minimum retention period, while remaining accessible to those who require access and are authorised to access that information.

In accordance with the Data Protection Act, personal data should not be retained for longer than it is required for the purposes for which it was collected.

Outsourcing and Third Party Suppliers

This applies to any member of the College Group who is considering engaging a third party to supply a service where that service may involve third party access to the Group's information assets. It also applies to any third parties who may have access to the Group's non-public information or systems for a specified purpose. This third party access could occur in a number of scenarios, common examples being:

- The use of cloud computing services
- When third parties are involved in the design, development or operation of information systems for a College
- When third party access to the Group's information systems is granted from remote locations where computer and network facilities may not be under the control of the Group
- When users who are not members of the Group are given access to information or information systems

Prior to outsourcing or allowing a third party access to the Group's non-public information or systems, a decision must be taken by staff of appropriate seniority that the risks involved are clearly identified and acceptable to the College. The level of staff seniority will depend on the nature and scale of the outsourcing. Advice should be sought from the Director of IT Services during the decision making process.

Where a service is formally outsourced by the College Group, the process must be managed by the relevant Group staff and a contract must be in place that covers standards and expectations relating to Information Security.

Third Party physical access

A risk assessment must be completed prior to allowing a third party to have access to secure areas of the College where confidential information and assets may be stored or processed. This assessment should take into account:

- What computing equipment the third party may have access to
- What information they could potentially access
- Who the third party is
- Whether they require supervision
- Whether any further steps can be taken to mitigate risk

Using personally owned devices

Any processing or storage of College Group information using personally owned devices must be in compliance with the College Group ICT Security Policy.

Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times. Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

Backups

IT Services will ensure that appropriate backup and system recovery measures are in place for Information that is entrusted to the care of IT Services. Where backups are stored off site/with a 3rd Party, appropriate security measures must be taken to protect against unauthorised disclosure or loss.

Exchanges of information

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Regular exchanges must be covered by a formal written agreement with the third party.