ICT and Information Security Policy

Policy Number	FCP2.47
Version Number	One
Status	Approved
Approval Date: first version	February 2015
Approval date: current version	February 2015
Responsible for policy:	Vice Principal – Finance
Responsible for implementation:	Vice Principal – Finance
Date of last review:	February 2015
Date of next review:	August 2017
Equality Impact Assessed	Yes
Committee Approval	JCC – 20 February 2015

Document Change History

Document Version	Section (No. or Heading)	Description of change(s)	Date of change
4			
3			
2			
1			

Contents

1 Introduction

This policy defines the College's approach to Information Security. It outlines relevant guidelines, policies and procedures currently utilised within Fife College and the critical roles and responsibilities expected of employees and students of the College in this area. The policy should be read in conjunction with Fife College's ICT Acceptable Use Policy. Non-compliance with this and other information security requirements may result in disciplinary action up to and including dismissal. In rare cases, a business case for non-compliance may be established; in all such cases the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a Department Manager and approved by the ICT department and the Senior Management Team (SMT).

2 Information Security Policy

2.1 Security Goals

The goal of the ICT and Information Security Policy is to ensure that information is treated correctly with regard to Confidentiality, Integrity and Availability regardless of the format in which it is held. For these purposes the following definitions apply:

Confidentiality - ensuring that information is accessible only to those authorised to have access.

Integrity - ensuring and safeguarding the accuracy and completeness of information and processing methods.

Availability - ensuring that authorised Users have access to information and associated assets when required.

The objective of this and associated policies and procedures are to maintain the security of information and to minimise business damage by preventing and controlling the impact of security incidents. Information security provides the essential framework in which information may be shared whilst ensuring the protection of that information.

This policy applies to all areas of College activity. This policy and those policies and procedures which support it must be adhered to by all staff. All other Users of College information and systems (including, for example, students, contractors and visitors) will be expected to adhere to policies to the extent to which their use, and degree of access to systems and facilities, is appropriate.

3 Principles for Information Security at Fife College

3.1 Risk Assessment

- Fife College's approach to security should be based on risk assessment.
- Fife College should continuously assess the risk and evaluate the need for protective measures as appropriate.
- An overall risk assessment of the information systems should be performed annually.
- Risk assessments must identify, quantify and prioritise the risks according to relevant criteria for acceptable risks.

- Risk assessments are to be carried out when implementing changes impacting information security.
- The system owners are responsible for ensuring that risk assessments within their area of responsibility are implemented in accordance with the policy.
- Risk management is to be carried out according to criteria approved by the management at Fife College.

3.2 Asset Management

- Assets include both information assets and physical assets.
- Information assets should be classified depending on the level of confidentiality.
- Fife College's physical ICT assets are governed by the Asset Management Lifecycle Policy.

3.3 Physical Security

- ICT equipment and information that require protection should be placed in secure physical areas. Secure areas should have suitable access control to ensure that only authorised personnel have access.
- The ICT Infrastructure and Networks Manager is responsible for approving physical access to technical computer rooms.
- Fife College's buildings should be physically secured when not in use.
- All external doors and windows must be closed and locked at the end of the work day.
- The appropriate manager should ensure that work performed by third parties in secure areas is suitably monitored to completion.
- ICT equipment must be protected against environmental threats such as fires, flooding, temperature variations etc.
- Sensitive information must not be stored on portable computer equipment (e.g. laptops, mobile phones, memory sticks, etc.). If it is necessary to store this information on portable equipment, the information must be password protected and encrypted with guidance from the College ICT department.
- Sensitive Information should not be stored within Cloud Storage systems unless these systems are part of the College network. Such information should reside within College Applications, or team and home drives.
- Secure areas and areas containing information systems must be secured with suitable fire extinguishing equipment with appropriate alarms.
- Fire drills shall be carried out on a regular basis.

3.4 Communications and Operations Management

Procurement and Installation

- All purchase and installation of ICT equipment, including Audio Visual equipment, must be approved by the ICT department.
- Purchase and installation of all software must be approved by the ICT department in accordance with the Software Evaluation process.

Documentation and Change Management

- The ICT department should ensure sufficient documentation of all the ICT systems.
- Changes in ICT systems should only be implemented according to the ICT department's Change Management policies and procedures.
- The ICT department should have taken precautions to be able to roll back from unsuccessful changes.
- Operational procedures should be documented to agreed standards. Documentation must be updated following regular review.
- Development, testing and maintenance should be separated from operations in order to reduce the risk of unauthorised access or changes, and in order to reduce the impact of errors on the production environment.

External Access, Protection and Back Up

- Before external Contractors, Consultants and Partners are permitted to access the College network, either remotely or on-site, they must obtain the specific written approval of the ICT department.
- ICT equipment must be safeguarded against virus and other malicious code. This is the responsibility of the ICT department.
- The ICT department is responsible for carrying out regular backups and restorations, as well as data storage on Fife College's ICT systems.
- Backups should include off-site or geographically dispersed copies that are stored in a secure manner.
- The ICT department has the overall responsibility for protecting Fife College's internal network.
- There should be an inventory containing all equipment connected to Fife College's wired networks.
- All access to Fife College's networks should be securely logged.
- Procedures and Guidelines for the management of removable storage media are available from the ICT Department.
- Storage media should be disposed of securely and safely when no longer required, using formal procedures.

Information Exchange and Privacy

- Procedures and controls should be established for protecting exchange of information with third parties and information transfer. Third party suppliers must comply with these procedures.
- Storage and transfer of sensitive information should be encrypted or otherwise protected.
- Users should have no expectation of privacy when using the network within the College. To manage systems, ensure security and compliance with appropriate College policies and procedures, the College ICT department may log, review, and otherwise utilise any information stored on, or passing through, the network. For these same purposes, the College may also capture User activity such as telephone numbers dialled and web sites visited.
- Information exchanged across public networks in connection with e-commerce will be protected as far as possible against fraud and unauthorised access and changes.

- The ICT department should ensure that publicly accessible information, e.g. on Fife College's web services, is adequately protected against unauthorised access.
- Access and use of ICT systems should be logged and monitored in order to detect unauthorised activities.
- Usage and decisions should be traceable to a specific entity, e.g. a person or a specific system.

Incidents

- The ICT department should record as appropriate substantial disruptions and irregularities of system operations, along with potential causes of the errors.
- Capacity, uptime and quality of the ICT systems and networks should be sufficiently monitored in order to ensure reliable operation and availability.
- The ICT department should log security incidents for all essential systems.
- The ICT department should ensure that system clocks are synchronised to the correct time.

3.5 Access Control

- Written guidelines for access control and passwords based on business and security requirements should be in place. Guidelines should be re-evaluated on a regular basis.
- Guidelines should contain password requirements (frequency of change, minimum length, character types which may/must be utilised, etc.) and regulate password storage.
- Users accessing systems must be authenticated according to specific guidelines.
- Users are responsible for any usage of their usernames and passwords. Users should keep their passwords confidential and not disclose them under any circumstances.
- Access to information systems should be authorised by line managers in accordance with the system owner directives.
- Access to information systems should be implemented in a way that provides the minimum privileges required for the User to perform their duties and responsibilities.
- The level of access given should be appropriate to the individual’s job function.
- The ICT department is responsible for ensuring that network access is granted in accordance with access policy.
- Users should only have access to the services they are authorised to use.
- Access to privileged accounts and sensitive areas should be restricted so that Users are prevented from accessing unauthorised information.
- Remote access to Fife College's computer equipment and services is only permitted if the Remote Access Policy has been read and understood and the ICT regulations signed.
- Remote access to Fife College's network may only take place through security solutions approved by the ICT department.
- College mobile devices should be protected using appropriate security measures.
- Information classified as sensitive must be encrypted if stored on portable media, such as memory sticks, DVDs and mobile devices.

3.6 System Development and Maintenance

- All changes to production environments should comply with ICT department policies and procedures.
- The implementation of changes to the production environment should be controlled by formal procedures for change management, in order to minimise the risk to data integrity, data loss or information systems.
- Systems developed for or by Fife College must satisfy defined security requirements, including data verification and robustness of code before being put in to production.
- All software should be thoroughly tested and formally accepted by the system owner and the ICT department before being transferred to the production environment.

3.7 Information Security Incident Management

- All breaches of security, along with the inappropriate use of information systems, should be treated as incidents.
- All employees are responsible for reporting potential or known breaches of security. Incidents should be reported to line managers or the Head of ICT Services.
- Procedures should be developed for incident management and reporting. The procedures should contain outcomes for preventing repetition of the incident as well as steps to undertake for minimising the damage.
- The appropriate ICT personnel should be familiar with procedures and tools for collecting evidence in the event of an incident.

3.8 Business Continuity Management

- An intermediate plan for continuity and contingencies covering critical and essential information systems and infrastructure should exist until the process of procuring a new Backup and Disaster Recovery solution(s) is complete.
- The continuity plan should be tested on a regular basis to ensure fitness for purpose, that it is kept up-to-date and to ensure that management and employees understand their roles in the event of a disaster.

3.9 Compliance

It is the policy of the College that all of its activities must be conducted in accordance with legislation. If any User of information is unsure as to their responsibilities in relation to the law they should seek advice through their line manager. The use of information is governed by a variety of different Acts of Parliament. These include but are not limited to:

- 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 Copyright, Designs and Patents Act 1988
- The Electronic Communications Act 2000
- Waste Electrical and Electronic Recycling (WEEE) regulations 2013

These various laws should be read together with various Statutory Instruments and other pieces of legislation with any associated upgrades, amendments and any new legislation enacted since the original date.