

# LONGLEY PARK SIXTH FORM COLLEGE

## ICT SYSTEMS SECURITY POLICY

Originator:	Derek Taylor, Network Manager
Date of Last Approval:	14 December 2005
Approval/review by:	Resources Committee/Corporation May 2011
Review interval (years):	3
Date of next review/approval:	May 2014

# LONGLEY PARK SIXTH FORM COLLEGE

## ICT SECURITY POLICY

### 1. Principle

- 1.1. To provide a framework for best operational practice to enable the College to maintain data integrity and security and to comply with all relevant legislation.

### 2. Introduction

- 2.1. ICT Systems play a major role in supporting the activities of the College. The success of the College is dependent upon the integrity and security of its data. Effective security is achieved by working with proper discipline, in compliance with legislation and by adherence to approved College Codes of Practice.
- 2.2. This ICT Security Policy and associated Codes of Practice set out the responsibilities for ensuring the security of ICT Systems within the College, and the procedures to be followed to safeguard the resources provided and the confidentiality and integrity of the information held thereon.

### 3. Scope

- 3.1. This Policy and associated Codes of Practice applies to:
  - all staff, students and visitors to the College. This includes contractors or authorised persons accessing the systems remotely
  - any system which captures, stores or processes information. This includes, but is not limited to, CCTV, desktop computers, laptop computers, telephones, voicemail, financial and staff/student records systems

### 4. Objectives

- 4.1. The objectives of this policy are to ensure that:
  - all of the College's ICT hardware systems, programs, data, network and equipment are adequately protected against loss, misuse or abuse
  - all users are aware of and fully comply with this Policy and are aware of, and work in accordance with, the relevant Codes of Practice
  - all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle

### 5. Compliance with Legislation

- 5.1. The College, and all users of its systems, have an obligation to abide by all UK legislation and relevant legislation of the European Community. Of particular importance in this respect are the following:
  - Regulation of Investigatory Powers Act 2000 (RIPA), together with Regulations issued pursuant to that Act, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, ~~which came into force in October 2000~~

- The Data Protection Act 1998, ~~which came into force in March 2000~~
- The Human Rights Act 1998, ~~which came into force in October 2000~~
- The Copyright, Designs & Patents Act 1988
- The Computer Misuse Act 1990
- Freedom of Information Act 2000

## 6. Responsibilities

- 6.1 It is the responsibility of each individual to ensure their understanding of, and compliance with this Policy and the associated Codes of Practice.
- 6.2 All College staff are responsible for the immediate reporting of any ICT security related incident to the Network Manager.
- 6.3 The CIS Manager shall take appropriate steps to inform staff, students and visitors of their obligations under this policy and any other policy referred to herein.
- 6.4 The College and its auditors will periodically review the adequacy of ICT system controls as well as compliance with such controls.

## 7. Breaches of Security

- 7.1 Security of the network systems and data is paramount. During the course of their normal duties, ICT Support staff may take action or make recommendations consistent with maintaining the security of College ICT Systems. Any breach of security of the College's ICT System could lead to loss of personal data and could be an infringement of the Data Protection Act 1998, leading to civil or criminal proceedings. It is vital, therefore, that users of College ICT Systems comply, not only with this policy, but also with the College's Data Protection Policy.
- 7.2 Any user suspecting a breach, or threat to ICT security should inform the Network Manager who will determine what action should be taken. In the event of a suspected or actual breach of security, the Network Manager may make inaccessible or remove any unsafe user or login names, data and/or programs on the system from the network, computer systems and any associated equipment, pending further investigation.
- 7.3 The Network Manager has the authority to take whatever action is deemed necessary to protect the College against breaches of ICT security. As far as is reasonably possible, any such action will be taken after consultation with the Principal or Vice Principal(s) **or Assistant Principal**.

## 8. Policy Awareness and Disciplinary Procedures

- 8.1 This policy is available on the College website and intranet. All users covered in section 3.1 will be made aware of the location of this policy.
- 8.2 Failure of an individual to comply with this policy and the associated policies and procedures referenced within it, may lead to the instigation of the relevant disciplinary procedures. In certain circumstances this may lead to legal action.

## 9. Associated Documents

### 9.1 Policies

- Disciplinary Policy - [http://www.longleypark.ac.uk/files/policy\\_documents/Disciplinary%20Procedure.pdf](http://www.longleypark.ac.uk/files/policy_documents/Disciplinary%20Procedure.pdf)
- Staff Code of Conduct - [http://www.longleypark.ac.uk/files/policy\\_documents/Staff%20Code%20of%20Conduct.pdf](http://www.longleypark.ac.uk/files/policy_documents/Staff%20Code%20of%20Conduct.pdf)
- Data Protection Policy - [http://www.longleypark.ac.uk/files/policy\\_documents/DPA%202010.pdf](http://www.longleypark.ac.uk/files/policy_documents/DPA%202010.pdf)
- JANET Acceptable Use Policy - <http://www.ja.net/documents/publications/policy/aup.pdf>
- ICT Systems Acceptable Use Policy - [http://www.longleypark.ac.uk/files/policy\\_documents/ICT%20Systems%20Acceptable%20Use%20Policy%20v2.doc](http://www.longleypark.ac.uk/files/policy_documents/ICT%20Systems%20Acceptable%20Use%20Policy%20v2.doc)

### 9.2 Regulations

- Regulation of Investigatory Powers Act 2000 – <http://www.legislation.gov.uk/ukpga/2000/23/contents>
- Data Protection Act 1998 – <http://www.legislation.gov.uk/ukpga/1998/29/contents>
- Human Rights Act 1998 – <http://www.legislation.gov.uk/ukpga/1998/42/contents>
- Copyright, Designs & Patents Act 1988 – <http://www.legislation.gov.uk/ukpga/1988/48/contents>
- The Computer Misuse Act 1990 – <http://www.legislation.gov.uk/ukpga/1990/18/contents>
- Freedom of Information Act 2000 – <http://www.legislation.gov.uk/ukpga/2000/36/contents>
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 – <http://www.legislation.gov.uk/uksi/2000/2699/contents/made>

### 9.3 Procedures

- ~~Managing Information Systems accounts – insert link to document when approved~~

## 10. Status

- 10.1 This policy does not form part of a formal contract of employment with the College, but it is a condition of employment that employees abide by this, and other College policies that have been approved by the Board of Governors. Likewise, the policy is an integral part of the Student Contract.

## 11. Review

- 11.1 This policy and associated procedures will be reviewed and tested ~~annually~~ every three years.