

## **ST MICHAEL'S COLLEGE**

### **COMPUTER SECURITY AND MISUSE POLICY AND PROCEDURE**

#### **STAFF AND STUDENTS**

##### **POLICY STATEMENT**

St Michael's College regards the integrity of its computer resources, including hardware, databases and software, as central to the needs and success of our day-to-day operations and longer term planning objectives. St. Michael's College policy is to take any measures it considers necessary to ensure that all aspects of the system are fully protected.

##### **POLICY APPLICATION**

The Computer Security Policy and Procedure applies to all staff and students. It is designed to protect individual data, corporate data, programmes, hardware and the network as a resource for the entire organisation. The following procedure and guidance sets out the rules and behaviours expected from all staff and students who manage and use the systems.

##### **PROCEDURE**

- Overall computer security is the responsibility of the Business Manager reporting to the Principal.
- Staff and students are permitted access only to those parts of the computer system which they need to enter in order to do their normal duties or studies. Levels of access will be decided by the Business Manager in consultation with the Principal.
- New permanent staff and all students will be questioned on their computer experience and will be given a copy of the Computer Security Policy and Procedure at their induction.
- Temporary staff will be checked in as much detail as possible before they are allowed access to the computer system. All such agency staff will be given a copy of the Computer Security Policy and Procedure.
- All staff and students will be trained in the use of St Michael's College computer resources as and when study or job requirements dictate.
- Access to the computer resources will only be gained through the use of a personal password. Such passwords must not be given to any other person and must be changed regularly as directed by the Information Officer. Passwords will only be issued on receipt of signed confirmation that staff members and students have read and understood St. Michael's College Computer Policy and Procedure.
- Those members of staff or students who have access to personal sensitive data must not divulge such information to a third party other than where directed by the Principal or the Police.

- All software used within St. Michael's College must be authorised by the Information Officer. Under no circumstances may any other software be installed.
- Staff and students are given access to the internet and e-mail facilities. The rules governing the use of these facilities are set out in the E-mail and Internet Policy. St. Michael's College expects its staff and students to restrict personal use of these facilities to a minimum.
- Staff and students should not have an expectation of privacy in anything created, stored, sent or received via the computer facilities. Without prior notice the Principal may review any material created, stored, sent or received on its network through the Internet, through e-mail or any individual computer.
- No game playing is permitted.
- Computer disks sent from external sources must be checked for viruses before use. Disks generated internally are the responsibility of the staff member who must store them in a secure place.

## **MISUSE**

Misuse of St Michael's College computer resources is a serious disciplinary offence. The following are examples of misuse:

- fraud and theft
- system sabotage
- introduction of viruses
- use of unauthorised software
- use of system for game playing
- excessive use of facilities for private purposes
- breaches of the Data Protection Act
- sending abusive, rude or defamatory messages via e-mail
- hacking
- breach of the policy and procedure

This list is not exhaustive. Depending upon the circumstances of each case, misuse of the computer system is likely to be considered gross misconduct punishable by dismissal. Misuse amounting to criminal activity may be reported to the police.

All breeches of computer security must be referred to the Principal.

Any member of staff or student who suspects that a colleague of whatever seniority is abusing the computer system may speak in confidence to the Principal or the Business Manager.

July 2010