Business School of Commerce and Management

Abuja, Nigeria

“Data Protection Policy”

E: info@bscm-edu.org

W: www.bscm-edu.org

Data Protection Policy

Policy Statement

Business School of Commerce and Management needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information stored in files (either paper based or electronically including on a computer including e-mail, internet, intranet or portable storage device) covered by the data protection legislation must be collected and used fairly, stored and disposed of safely and not disclosed to any other person unlawfully.

To do this, the Centre must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not to be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The Centre and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Centre has developed the Data Protection policy.

Scope

This policy applies to all members of the Centre community (staffs, students, contractors/suppliers and members of the public).

This policy does not form part of the formal staff contract of employment nor of the student contract with the Centre, but it is a condition of both that the rules and policies made by the College will be complied with. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any members of staff or students who consider that the policy has not been followed in respect of personal data about themselves or about other data subjects should raise the matter with the designated data controller initially (students may wish to do this through their lecturer or course tutor). If the matter is not resolved it should be raised as a formal complaint or grievance or through the College's Public Interest Disclosure Procedure where appropriate.

Notification of Data Held and Processed

- All staff, students and other data subjects are entitled to
    - Know what information the College holds and processes about them and why
    - Know how to gain access to it
    - Know how to keep it up to date
    - Know what the College is doing to comply with its obligations under the
- 1998 Act
- The Centre will advise staff and students and other relevant data subjects about the types of data the Centre holds and processes about them, and the Reasons for which it is processed. This will be notified via application/enrolment or other documentation.

Legislation

- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Education Act 2002
- Mental Capacity Act 2005

Responsibilities

All staff is responsible for

- Checking that any information they provide to the Centre in connection with their employment is accurate and up to date.
- Informing the Centre of any changes to information which they have provided, e.g. change of address.
- Checking the information that the Centre will send to them from time to time, giving details of information kept and processed about them.
- Informing the Centre of any errors or changes. The College cannot be held responsible for any errors which staff members have had the opportunity to correct.
- If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students' course work, opinions about ability, references to

other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are at appendix 1.

- The Data Controller and the Designated Data Controller. The College as a body corporate is the data controller under the Act and the board of governors is therefore ultimately responsible for implementation.

Actions to Implement and Develop Policy

- **Data Security**

All staff are responsible for ensuring that:
· Any personal data which they hold are kept and disposed of securely.
· Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
Personal information should be
· Kept in a locked office, or
· In a locked filing cabinet, or
· In a locked drawer, or
· If it is computerised, be password protected, or
· Kept only on disk or other portable device which is itself kept securely

- **Unauthorised Access**

Any member of staff or student who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party may be disciplined in accordance with Centre procedures.

- **Student Obligations**

Students must ensure that all personal data provided to the Centre are accurate and up to date. Students must ensure that changes of address, etc, are notified to operation Director.

- **Rights of Access to Information**

Staff, students and other data subjects have the right of access to any personal data that are being kept about them either on computer or in certain other files. Any person who wishes to exercise this right should complete the Centre "Access to Information" form and give it to the designated data controller or, in the case of a student, to her/his course tutor or lecturer. Forms are available from the designated data controller.

- **Public Domain**

Information that is already in the public domain is exempt from the 1998 Act.

- **Subject Consent**

In many cases, the Centre can only process personal data with the consent of the individual. In some cases, if the data are sensitive, express consent must be obtained. Data are considered sensitive if they are about an individual's race; political opinions; religious beliefs; trade union membership; health; sex life or criminal record.

Agreement to the Centre processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous convictions. The College also has a duty of care to all staff and students and must therefore make sure those employees and those who use the College facilities do not pose a threat or danger to other users.

- **Examination Marks**

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned.

- **Retention of Data**

A full list of information with retention times is available from the designated data controller and detailed in the Archive policy retention schedule. The Centre will keep some forms of information for longer than others. In general information about students will be kept for a maximum of ten years after they leave the Centre.

Some information, including information about health, or disciplinary matters will be destroyed within 3 years of the students leaving the Centre. The Centre will need to keep information about staff for six years after the member of staff leaves. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, health, potential or current disputes or litigation regarding the employment and information required for job references.

- **Monitoring & Evaluation**

The designated data controller will monitor and evaluate the policy by submitting a report annually to the College Management Team.

- **Related Policies**

· Admissions Policy

Staff Guidelines for Data Protection

- All staff has a duty to make sure that they comply with the data protection principles. In particular, staff must ensure that records are:

· Accurate
· Up to date
· Fair
· Kept and disposed of safely, and in accordance with Centre policy

- Information about a data subject's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the subject's consent. e.g. recording information about dietary needs for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant as part of pastoral duties.

- Before processing any personal data staff should consider the checklist below:

Checklist for Processing Data

· Do you really need to record the information?
· Is the information 'standard' or is it 'sensitive'?
· If it is sensitive, do you have the data subject's express consent?
· Has the data subject been told that this type of data will be processed?
· Are you authorised to collect/store/process the data?
· If yes, have you checked with the data subject that the data are accurate?
· Are you sure that the data are secure?
· If you do not have the data subject's consent to process, are you satisfied that it is in that person's best interests to collect and retain the data?
· Do you have the data subject's consent before you disclose the data to a third part?