DATA PROTECTION POLICY

1. Policy Statement

1.1 The British University in Egypt is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and others) in accordance with recognized UK Data Protection principles, and in keeping with the requirements of Egyptian law and expectations regarding cultural norms. The University needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, to comply with contractual obligations to validating bodies, and to comply with legal obligations to the government). Information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party inappropriately.

2. Legal Framework

2.1 The UK Data Protection Act (DPA) (1998), which determines the policy of BUE's UK partners in relation to the management of personal data, does not apply in Egypt.

2.2 Egyptian Labour Law article 56 states: “the worker is obliged to keep and maintain work secrets and not to disclose any information pertaining to work as long as it is secret per se or upon written instructions issued from the Employer”. In this context, personal employee data are considered work secrets.

2.3 Custom and practice dictate that disclosure of personal data to third parties is unacceptable. It is, however, considered acceptable for immediate family members, such as parents, guardians...etc to expect full and free access to students' academic data pertaining to their performance in their relevant programmes. (Refer to 5. Data Protection Principles)

3. BUE's Approach

3.1 The approach taken by the BUE, given the environment described in 2 above, is to adopt and adapt the relevant DPA principles, as benchmark standards of good practice, taking into account the Egyptian legal and cultural context. The University, as the owner of personal data, considers that it has a duty of care to its
data subjects to protect their privacy and interests by sensitive handling of their records.

4. **Definitions** *(adapted from the DPA)*

4.1 **Personal Data:** Data relating to a living individual who can be identified from that information or from that data and other information in possession of the authorised individuals, including name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the authorised person in respect of that individual.

4.2 **Sensitive Data:** Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

4.3 **Data Subject:** Any living individual who is the subject of personal data held by an organization.

4.4 **Processing:** Any operation related to organization, retrieval, disclosure and deletion of data and includes: obtaining and recording data; accessing, altering, adding to, merging, deleting data; retrieval, consultation or use of data; disclosure or otherwise making available of data.

5. **Data Protection Principles**

All processing of personal and sensitive data must be done in accordance with the principles below:

5.1 **Data shall be processed fairly and according to the levels of subsystems & underlying application detailed in the "Management Structure for the SRS" document.** Those responsible for processing data must make reasonable efforts to ensure that data subjects are informed of the identity of the authorised individual, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

5.2 **Data shall be obtained for specific purposes by authorised individuals as detailed in the "Management Structure for SRS" document and not processed in a manner incompatible with those purposes.** Data obtained for specified purposes must not be used for a purpose that differs from those.

5.3 **Data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.** Information which is not strictly necessary for the purpose for
which it was obtained should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed: this is the responsibility of the authorised person accessing the information.

5.4 Data shall be accurate and, where necessary, kept up to date. Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the University are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the University of any change in circumstances to enable personal records to be updated accordingly. It is the responsibility of the University to ensure that any notification regarding change of circumstances is noted and acted upon.

5.5 Data shall be kept only for as long as necessary and as detailed in Point 9.3

5.6 Sensitive data shall not be disclosed to any third party unless required by law to do so.

5.7 Appropriate technical and organizational measures shall be taken against unauthorised processing, accidental loss or destruction of data.

6. Data Subject Rights

Data subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed (an administrative fee may be charged for such information, as approved and announced by the University).
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision making process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To take action to rectify, block, erase or destroy inaccurate data.
7. Consent

7.1 Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent to the University and/or the inquiring agency. The University understands “consent” to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7.2 In most instances consent to process personal and sensitive data is obtained routinely by the University (e.g. when a student signs a registration form or when a new member of staff signs a contract of employment). Any University forms (whether paper-based or web-based) that request data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed.

7.3 If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

7.4 The above guidelines of consent are applicable to the BUE Email policy which is published separately.

8. Security of Data

8.1 All staff are responsible for ensuring that any personal data (on others), which they hold, are kept securely and are not disclosed to any unauthorised third party.

8.2 All personal data should be accessible only to those who need to use it. Authorised Personnel should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerized, password protected, or
- kept on disks which are themselves kept securely.
8.3 Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers. Manual records should not be left where they can be accessed by unauthorised personnel.

8.4 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as “confidential waste”. Hard drives of redundant PCs should be wiped clean before disposal.

8.5 This policy also applies to staff and students who process personal data “off-site”. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside the University campus.

9. Retention and Disposal of Data

9.1 The University discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and students. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

9.2 Students

In general, electronic student records containing information about individual students are kept indefinitely and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained.

Authorised Department Staff -as detailed in the Management Structure of the SRS Document- should regularly review the personal files of individual students in accordance with the University’s Records Retention Schedule.

9.3 Staff

In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by the HR Department for 6 years from the end of employment.

Departments should regularly review the personal files of individual staff members in accordance with the University’s Records Retention Schedule.
Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. HR may keep a record of names of individuals that have applied for, been short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

9.4 Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

10 Disclosure of Data

Personal data may be legitimately disclosed where one of the following conditions apply:

- the individual has given their consent (e.g. a student / member of staff has consented to the University corresponding with a named third party);
- where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff – personal information that can be disclosed to other University employees if it is clear that those members of staff shall require the information to enable them to perform their jobs);
- where the institution is legally obliged to disclose the data;
- where disclosure of data is required for the performance of a contract.