DATA PROTECTION POLICY

1. - CODE OF PRACTICE AND PROCEDURE

The Data Protection Act 1988 (DPA) imposes legal obligations on universities with regard to the storage and use of personal data and its security. All who use personal data must register with the Data Protection Register (DPA). 'Personal Data' is defined as any information identifiable to living individuals. Data protection legislation is designed to control how personal information is used by organisations, businesses or the government. All personal information disclosed or otherwise provided to the University of Buckingham will be subject to the terms of the University Data Protection Policy. Therefore, it is expected that all members of staff and students will comply with this policy. Failure to comply may result in individual prosecution as well as prosecution of the University.

1.1. - What data is held and where data is held?

The DPA covers information contained in any format. Therefore it is good practice to assume that all manual/electronic paper records of personal data, both staff and student, held by the University are covered.

The University holds and processes the following information: personal details; academic records; finance details; disabilities; medical reports; information on criminal records; University disciplinary action; GMC Fitness to Practice panels (N.B. the examples are not exhaustive and are for guidance only).

The general rule is that manual/electronic records must be kept securely. The information that the University holds about staff and/or students will be kept in both manual and automated systems. For instance, personal information relating to staff at the University of Buckingham can be found on the Human Resources system (Ciphr), the Finance system (QLX) and the Payroll system (ActionFile). Personal information relating to University of Buckingham students can be found principally in the Student Records System (SITS), the Finance System (QLX), and the Extended Medical Examination Record (EMER). The Central Student Welfare stores data centrally in the Student Records System (J drive) and/or in locked cabinets within the department. Some of this data is shared, with the student's consent, among the relevant Schools who keep the data in a designated system/drive. Medical records for MBChB students are held by the Occupational Health Department in Milton Keynes. These are held in the Occupational Health Service (OHS) NHS database and no paper versions are maintained, the database is secure and only accessible by OHS staff.

All data and information about staff and students contained in these systems, and elsewhere is subject to the DPA and must be handled in accordance with the terms of the DPA and this policy.

Questions about adherence to this policy should be directed to the University Data Protection Officer.

1.2. – Data Protection Principles

The Act establishes a code of practice outlined in the following eight enforceable principles. These principles have been elaborated and explained by the Information Commissioner Officer (ICO) as follows:

Principle 1: Processed fairly and lawfully.

In practice, it means that the University must:

- have legitimate grounds for collecting and using personal data;
- not use the data in ways that have unjustified adverse effects on the individual concerned;
- be transparent about how it intends to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
  ensure it does not do anything unlawful with the data.

Principle 2: Processed for the limited purposes specified in the data user's register entry and not in any manner incompatible with those purposes.

In practice, it means that the University must:

- be clear from the outset about why it is collecting personal data and what it intends to do with it;
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- comply with the Act regarding notifying the Information Commissioner;
- ensure that if it wishes to use or disclose the personal data for any purpose that is additional to, or different from, the originally specified purpose, the new use or disclosure is fair.

Principle 3: Adequate, relevant and not excessive for those purposes.

In practice, it means the University should ensure that:

- it holds personal data about an individual that is sufficient for the purpose it is holding it for, in relation to that individual;
- it does not hold more information than is needed for that purpose.

Principle 4: Accurate and up-to-date.

It means that the University should:

- take reasonable steps to ensure the accuracy of any personal data it obtains;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of the information; consider whether it is necessary to update the information.

Principle 5: Not kept longer than necessary for the specified purposes.

In practice, it means that the University will need to:

- review the length of time it keeps personal data;
- consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; update, archive or securely delete information that is out of date.

Principle 6: Processed in line with the data subjects' rights.

The rights referred to are:

- a right of access to a copy of the information comprising their personal data (see chapter on subject access requests);
- a right to object to processing of data that is likely to cause or is causing damage or distress;
- a right to prevent processing of data for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- a right to claim compensation for damages caused by a breach of the Act by the University.

Principle 7: Properly protected against loss or disclosure.

In practice, it means that the University must have appropriate security to prevent the personal data it holds from being accidentally or deliberately compromised. In particular, it will need to:

- design and organise its security to fit the nature of the personal data it holds and the harm that may result from a security breach;
- be clear about who is responsible for ensuring information security;
- make sure it has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff;
- be ready to respond to any breach of security swiftly and effectively.

Principle 8: Not transferred to countries outside the UK without adequate protection.

Personal data must not be transferred to a country outside the European Economic Area unless:

- explicit consent has been obtained from the individual(s);
- the data has been completely anonymised;
- that country ensures an adequate level of protection for data subjects;
- a contract is in place with the recipient of the personal data, which puts the necessary safeguards in place.

All members of staff and students should ensure that they observe this code.

1.3- Access Requests to staff and/or student records

Under Section 7 of the Data Protection Act individuals have rights of access to information held by the University through a 'subject access request'. All requests should be made to the School holding the information. The University will charge an administration fee of £10 bearing in mind that special rules apply for paper based health records and education records to a maximum fee of £50.

All subject access requests should be in writing and should include a full name, address and contact telephone number; any information used by the School to identify or distinguish the individual; details of the specific information required and any relevant dates.

In most cases a response to a subject access request will be within 40 calendar days of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request.

1.4. - Retention Period

The University of Buckingham will retain personal information as long as it is operationally necessary to do so –even beyond the termination of the student affiliation.

It is however recommended that student files are held for a period of 7 years after the student leaves the University. After this period the records are considered no longer relevant and should be destroyed. The exception to this is academic records (i.e. mark and grades attained) which are retained permanently.

Staff records, health and safety and library service are recommended to be held for a period of 5 years.

1.5. - Disclosure: Release of Personal Information to a Third Party

In accordance with legal obligations for the fair and lawful processing of information the processing of personal data includes various safeguards for the individuals concerned. Unauthorised disclosure to third parties is prohibited, unless such a disclosure is permitted or required under the DPA.

These exemptions relate to matters where disclosure is required by law or is necessary in connection with legal proceedings. Therefore, if the University of Buckingham receives a request from a third party for information constituting personal data, it may be required to release the data to the third

party without the knowledge or consent of the data subject. Before any such release, the University must be satisfied that an exemption applies.

a) Disclosure to the police

Disclosure is NOT compulsory except in cases where the University is served with a Court Order requiring such information.

On occasions, the Police may require personal data on students and/or staff for the purposes of prevention or detection of crime and/or the apprehension or prosecution of offenders. Personal information of this nature is exempted from the normal rules on data protection by Section 29(1) and (3) of the DPA. The University is under a legal duty to disclose such information to the relevant police authority.

However, the information requested should be in the appropriate format i.e. an official form must be submitted (most Police Forces will have their own request form) which should contain the following information: name of the Police Force requesting the information; a statement confirming that the information requested is required for the purposes covered in Section 29 DPA; a brief outline of the nature of the investigation; the student or staff member's role in that investigation; the name, signature and identification number of the Investigating Officer. Staff must not release information to the Police over the telephone.

b) Legal Proceedings and Legal Advice

Section 35(2) of the DPA exempts data from the non-disclosure provisions (e.g. obtaining consent from student or staff) in cases where disclosure is necessary "for the purpose of, or in connection with, legal proceedings…or for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights". In such instances, data can be released. Any release of data under this exemption must be approved by the Data Protection Officer.

c) Regulatory Activity

Section 31 of the DPA provides the release of personal data for the purpose of certain functions. Therefore, the University needs to comply with certain bodies that regulate the profession or occupation concerned for. In other words, where particular degree schemes lead to professional recognition, accreditation or exemption, students' final result, including any failures, will be communicated to the relevant professional body. Moreover, the University of Buckingham will release information to a third party if it has a statutory right of access, such as establishing whether a student is "fit to practise". A release of information under this provision does not require approval of the University Data Protection Officer.

d) Other External Bodies

Personal data should not be given outside the University without consent or justification. However, the University is required to provide information to other external bodies such as Higher Education Statistical Agency, Grant Awarding Bodies, Student Loan Company, Local Authorities for Council Tax and Electoral Roll purpose and the Home Office.

e) Other requests

Family members: the University has no obligation to disclose information about a student or member of staff to family members or friends.

Sponsors and/or sponsoring bodies: in the student declaration form (see General Regulation 1.2), a copy of which students sign on registration, students confirm that they are aware that personal data is to be released and to whom e.g. students have agreed to disclose their results and details to sponsors.

References: the writer of a reference may stipulate that it shall be confidential, and the writer need not show it to the individual about whom it is written. The information released should be the minimum relevant to the request – usually attendance and award details, classification and module marks. A response should only be made to requests received in writing. References provided by the request of a student are considered to be provided with the consent of the student, and thus, do not require a consultation and approval of the University Data Protection Officer.

2. – GUIDANCE FOR STAFF AND RESEARCH STUDENTS

2.1. - Student status is regarded as personal data and thus, to be processed in accordance with the DPA and this policy. For example, by confirming whether or not an individual is (or has been) registered at the University could be a breach of the Act.

Therefore, when a request for confirmation of student status, do please exercise caution before responding. Do always employ appropriate security measures to check the identity of the enquirer and, do not disclose information over the telephone. Wherever possible, ask the enquirer to put their request in writing, preferably on headed paper and if necessary, subject to approval by the University Data Protection Officer

2.2. - Photographs and/or film for display: members of staff and/or students may be photographed and/or filmed as part of group scenes in classes, whilst on campus and/or open days. Such footage may be used by the University in the production of promotional material such as the prospectus.

Small Groups/Individuals: if the main subject, consent is needed before any photographs are taken.

- The consent form: ensure that students are informed of what the images will be used for (e.g. where the photos will be displayed, who will have access to them).

- If a department wishes to prepare a poster of photos and/or names of the students taking courses for display on a notice board there is the need to give consent (unless this has already been granted – check the consent form).

- Taking photos from the SIC platform (to distribute): check at the consent form – the question you need to ask is: for what purpose are you doing so? If it is covered in the consent form e.g. academic purposes such as to be easily identifiable to a lecturer, then you do not need permission.

- Photographs/film on the Web/online: to be restricted to Intranet (not be used on the Internet). The internet is a global instrument and it transfers personal data outside of the EU. That

said, rules are much stricter and explicit consent for this particular purpose should be obtained from the student.

2.3. - Electronic devices AND electronic information (including data storage): personal information on staff or students which is retrieved/viewed using Staff Remote Access MUST NOT be stored on private computers or made accessible to students or any other member of the general public. In the event that personal information is to be consulted as a hard copy, such copies must be held securely whilst in use and all relevant information shredded at the earliest opportunity.

2.3.1- Personal information contained on <u>laptops or USB sticks.</u>

There may be occasions, when staff and/or students may be obliged to leave the University with personal information relating either to fellow staff members and/or students OR sensitive research data. If this is the case, then the staff member and/or student must fulfil two criteria:

a) They must have prior permission in writing to take this personal information off-site from their Dean /Head of Department; AND

b) Such information MUST be encrypted.

Simply having a password to the laptop or other device is not compliant with the DPA. If the laptop or device is stolen and the personal information becomes known, then the University could be liable to a fine of up to £500,000. Staff and/or students requiring University owned laptops to be encrypted should contact IT Services.

2.3.2- Personal information received by staff members and/or students <u>on email/tablets/smartphones</u>

Personal information sent to such devices should be encrypted. Generally, if one can receive personal information via e-mails on one of these devices it is expected to exercise the highest level of discretion and vigilance at all times when receiving and reading such information off-campus. Staff and/or students should ensure that their personal laptops/smartphones/tablet devices are not left in places where they could be viewed by others. Do refrain from opening e-mails containing personal information on fellow staff/students or personal research data in places like cafes or bars around the University, or on public transport.

2.3.3- Protecting personal information on members of staff PCs

It is important that all staff (academic and administrative) who deal with students and regularly have students in their offices (i.e. for tutorials) should lock their PCs or log off their PCs before leaving their workstation unattended for short periods. In addition, when leaving their offices during working hours, staff should ensure that their doors are locked at all times.

For more information in this matter see 'Use of University Computers and Data Networks (including Email Policy)'

With regard to cloud storage, the same 8 principles of the Data Protection Act are relevant.

Particular attention should be paid to principle 8 which refers to sending personal data outside the European Economic Area. Therefore, bear in mind that many of the popular cloud storage servers are based in other jurisdictions and they cannot be considered to offer adequate level of protection. The University provides enough storage and remote access which fits within the DPA and thus for your University data, the University's IT service should be used."

Patricia Covarrubia

Data Protection Officer

November 2015