Data Protection Policy

Effective Date: July, 2014

Contents

Appendix

1 Introduction

The University holds and processes information about its staff, students and other data subjects for academic, administrative and commercial purposes and also to fulfil statutory obligations to the government and other statutory bodies.

This policy should be read in conjunction with **Data Quality Policy** as all staff must make every effort to ensure that any data collected or entered into our systems is accurate, valid, reliable, timely and relevant.

2 The Eight Principles of Data Protection

When handling such information, the University and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the Act), as follows:

1. processed **fairly** and lawfully;
2. processed for **specific purposes** and in an appropriate manner;
3. adequate **relevant** and not excessive;
4. **accurate** and up-to-date;
5. not kept for longer than necessary;
6. processes in accordance with the rights of the data subjects;
7. protected by appropriate **security**;
8. not transferred outside the European Economic Area without adequate controls.

Common questions on the DPA and related issues can be found at

http://www.ico.gov.uk/Global/faqs.aspx.

'Personal data' is defined as data relating to a living individual who can be identified from that information, or from that data and other information in the possession of the data controller, or likely to come into the possession of the data controller. These include expressions of opinion about the individual and of the intentions of the data controller in respect of that individual. The individual may be a past, present, or potential member of staff, student, contractor, supplier, contact, referee, friend, or family member.

Processing personal data (including simply holding information about someone) is allowed only if **one** of the following conditions exists:

i.) With consent;
ii.) To perform a contract with the individual;
iii.) Under a legal obligation;
iv.) To protect the vital interests of the individual;
v.) To carry out public functions; or
vi.) To pursue the *legitimate* interests of the data controller unless prejudicial to the interests of the individual.

It is thus expected that for most purposes, item six will cover most of the needs of the University, but we must be careful of 'legitimacy'. The Information Commissioner advises us that

we do not need to add consent to the student enrolment form as long as we can justify the need for all of the data requested for our legitimate business processes.

The processing of sensitive personal data is subject to much stricter conditions. '**Sensitive personal data'** includes information relating to racial or ethnic origin, disability, political opinions, religious beliefs, trade union membership, health, sex life, and criminal convictions. Processing of sensitive personal data **also** needs **one** of the following:

i.) With explicit consent;
ii.) Under a legal obligation in the context of employment;
iii.) To protect the vital interests of the individual where consent cannot be given or is withheld;
iv.) By certain non-profit bodies about their members;
v.) Where the information has been made public;
vi.) In legal proceedings;
vii.) To carry out certain public functions, and
viii.) For medical purposes.

It is expected that we would need to gain explicit consent for this type of data, and keep robust records of this consent.

3 Processing of Personal Data

The University will hold the minimum personal data necessary for it to perform its functions, and the data will be erased once the need to hold it has passed in accordance with the recommended retention periods. Wherever possible, manual or computerised personal data will be held in one location only, with a named responsible person, to assist compliance with the Act. This will provide for improved security of data, consistency of data sets, ease of access for data subjects and confirmation of explicit (written) consent for sensitive data or that transmitted outside the EEA.

Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected without undue delay. Personal data will be treated as confidential. Sources and disclosures of personal data must be in accordance with the provisions of the Act and the University's notification under it. The University will make explicit on all appropriate documentation, which data is being requested for statistical monitoring only, for example, equal opportunities monitoring.

Unlike other acts of Parliament, individuals as well as University's can be prosecuted for breaches of the Act. Whilst employment with the University carries with it certain indemnities, special care must be taken to ensure compliance with the Act.

Other than for the purposes of "normal" University business or as a result of a statutory or legal obligation, personal data must not be disclosed to an unauthorised third party. There is no finite definition of "third party" but this could be taken as a person, persons or University who were not the intended recipient of the information and have no obvious reason for needing to know. Where a third party requests certain information, no data should be released until the identity of the third party has been carefully verified.

Where students enter into a contract/agreement with a third party employer, either paid or voluntary, personal data will be disclosed from the University under the terms of the Act. More information on the detailed information on the data exchanged can be found in the Student Handbook.

The University will keep different types of data for differing lengths of time, depending on legal, academic and operational requirements.

The University will take all reasonable steps to provide training and guidance in the use of personal data and will review its systems and procedures accordingly.

4 Responsibilities

The University as a corporate body is the Data Controller. The Senior Officer responsible for the Data Controller compliance is the Data Protection Officer. The University's Data Protection Officer oversees the implementation of the Data Protection Policy in accordance with the provisions of the Data Protection Act 1998. The Data Protection Officer for the University is the **Head of IT.** In the first instance, Subject Data Access Requests should be made in writing to the Data Protection Officer who will ensure the appropriate areas respond to requests.

All staff and students are expected to comply with this policy and any associated University guidelines or instructions. Breaches of the policy may constitute misconduct for which disciplinary action may be taken in accordance with the University's disciplinary procedures.

Any member of staff or student who considers that the Data Protection Policy has not been followed in respect of personal data about him- or herself, should raise the matter with the Data Protection Officer or HR Services Director initially. If the matter cannot be resolved informally then staff and students have recourse to the Staff Grievance Procedure or the Student Complaints Procedure respectively.

Data subjects (staff and students) have a responsibility for ensuring that

- All personal information which they provide to the University in connection with their employment/registration is accurate and up-to-date;
- The University is informed of any changes to the information which they have provided, for example, a change of address;
- The information that the University may send out from time to time, in written or automated form, is checked and any errors or changes notified as appropriate.

The University will make a charge of £10 for each official Subject Access Request under the Act, except for current staff and students.

The University aims to comply with requests for access to personal data within ten working days, but will ensure that it is provided within the 40 calendar days required by the Act.

5 Monitoring

The University may monitor staff and students by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, the University will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about him/her. The University will not retain such data for any longer than is absolutely necessary.

In exceptional circumstances, the University may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the University by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means (for example, where an employee is suspected of stealing property belonging to the University). Covert monitoring will take place only with the approval of Data Protection Officer.

6 Employee obligations regarding personal information

If an employee acquires any personal information in the course of his/her duties, he/she must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so;
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.

In particular, an employee should ensure that he/she:

- uses password-protected and encrypted software for the transmission and receipt of emails;
- sends fax transmissions to a direct fax where possible and with a secure cover sheet; and
- locks files in a secure cabinet.

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an employee acquires any personal information in error by whatever means, he/she shall inform [name of individual/the data protection officer] immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within the University.

Where an employee is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact data protection officer.

An employee must not take any personal information away from the University's premises [save in circumstances where he/she has obtained the prior consent of the senior manager to do so].

If an employee is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from their line manager. If he/she cannot get in touch with the senior management or the data protection officer, he/she should not disclose the information concerned.

7 Consequences of non-compliance

All employees are under an obligation to ensure that they have regard to the eight data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the University will treat this as gross misconduct and may instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

8 Taking employment records off site

An employee must not take employment records off site (whether in electronic or paper format) without prior authorisation from the data protection officer/senior management.

An employee may take only certain employment records off site. These are documents relating to

- disciplinary or grievance meetings that cannot be held on site
- meetings with occupational health/discussions
- surrounding the sale of the business
- or specific monitoring purposes/seeking professional advice

An employee may also take employment records off site for any other valid reason given by the Data Protection Officer/HR Services Director.

Any employee taking records off site must ensure that he/she does not leave his/her laptop, other device or any hard copies of employment records on the train, in the car or any other public place. He/she must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that inform.

9 Review of procedures and training

The University will provide training to all employees on data protection matters on induction and on a regular basis thereafter. If an employee considers that he/she would benefit from refresher training, he/she should contact Learning and Development Unit.

The University will review and ensure compliance with this policy at regular intervals.

10 Retention of Records

Under the Data Protection Act, personal data processed for any purposes shall not be kept for longer than is necessary for that purpose or those purposes. To prevent unauthorised or accidental disclosure of the information, it is essential to exercise care in its disposal, including protecting its security and confidentiality during storage, transportation, handling and destruction.

Faculties and departments must establish procedures appropriate to the information held and processed by them, and ensure that all staff are aware of those procedures. In addition, a disposal record should be held to assist the University in responding to any enquiries made under the Data Protection Act.

Detailed tables outlining current records and retention guidelines can be found on blackboard

http://bucks.ac.uk/formal/records

11 FAQs and Further Information

Anything I do at work is covered by corporate indemnity, isn't it?
No, individuals can be prosecuted for breaches of the Act.

Can I let parents or possible employers know about a student?
No. You must get written consent from the student to disclose any information.

What about medical emergencies?
You can disclose information in a medical emergency.

What about requests from the police?
The police must provide a 'section 29' form signed by a senior police officer, or a Court Order, before you can release information.

Can we have lists of students to invite them to join my club, or to offer them the chance to buy something?
No, unless they have 'opted in' to receive information of this type.

Can I put all my staff or student photos on the website?
Only if they have given written consent.

Is it alright to take information about students or staff home to work on?

Only in connection with your normal work and for no other purpose. You should take all reasonable precautions to ensure the security of the information entrusted to you, including that on paper, laptop or pen drive.

Can I see a reference you have written about me?

No, but the person who receives it must show you it if you ask.

Can I share statistical data?
Data can be shared as long as no individual can be identified in it.

When can students expect their examination marks?
Examination marks are exempt from subject access requests for the purpose of determining the results of an examination for forty days from the date of the announcement of the final result or five months from receipt of the request, whichever is sooner. This prevents students requesting access before all the marks have been finalised, but also takes the view that results should not take an inordinate time to be published.

Students are entitled to information about their marks for both course work and examinations. All students' results will be displayed publicly by ID number only, including provisional and part assessments. In the event that the full course fees have not been paid, or books or equipment have not been returned, results cannot be withheld but the University may not allow the student to re-enrol, graduate or receive certificates.

Do I have to show a student what I have written on their exam script if they ask?
Yes.

Do I have to show anybody anything I have written about them in my diary, or email?
Yes.

What about if we are in the middle of negotiations?
You do not have to disclose during the negotiation, but you will have to afterwards.

Does research have any special privileges?
Yes. Personal data used for research is exempt, as long as it is not processed to support measures or decisions with respect to an individual nor in a way likely to cause damage or distress to an individual. In such circumstances the processing is not to be regarded as incompatible with the purposes for which they were obtained. The personal data may be kept indefinitely, and the personal data are exempt from subject access rights provided that the results of any research or statistics are not made available in any form that identifies the data subjects.

Can I have access to the information you have on me on IT's back-up tapes?
No. Back-up data is exempt from subject access requests if it is only held for back-up purposes.

Where can I get further information?
Further general information is also available on the Information Commissioner's website:

http://www.informationcommissioner.gov.uk/data protection

Appendix 1

Guidance on Writing References for Students

The following guidance notes are intended for the advice of staff who may be asked to give references for current or past students. Being an academic referee is normally part of the role of the personal tutor, although all academics need to be aware that students might name them as their referee.

Responsibility

Type of reference	**Responsibility**	**Document**
Confirmation of Status- student/former student	Student Centre, AQD or Faculty PSEs	Headed paper
Personal/academic reference – student/former student	Appropriate academic e.g. personal tutor or dissertation supervisor	Non-headed paper
Pro-forma reference student/former student	*Factual sections* – Student Centre, AQD or Faculty PSEs depending on the information required *Comments* - Appropriate academic e.g. personal tutor or dissertation supervisor	Pro forma provided by potential employer

After 6 years of the student leaving the University, it may no longer be appropriate to provide a personal or academic reference, but just provide a Confirmation of Status.

The Confirmation of Status should contain:

- Name
- Dates of study at the University
- Title and duration of course
- Outcome of study where known (e.g. class of degree)

General Principles

- Do not supply any sensitive personal data as defined by the Data Protection Act (health, racial or ethnic origin, political opinions, religious beliefs, trade union membership, sex life, criminal convictions) without the explicit written permission of the student. A statement such as “I am not in a position to comment regarding X's health/sickness record." would be a suitable response.
- References should not include anything that you would not be prepared to show the individual you are writing about. Under the Data Protection Act students have the right to view a submitted reference.
- References can be **corporate** (e.g. concerning a current or former student and containing information relating to University records) or **personal** (e.g. written as a result of personal knowledge). Personal references provided in a private capacity should not be written on University headed paper.
- If you are challenged about a reference you must never admit liability. The matter should be referred to the Student Centre in the case of a student reference. Copies of references should be kept on the relevant faculty student file, ideally in electronic format.

- If you receive a request for a reference but are unable or unwilling to give it you must ensure the refusal is communicated carefully to avoid implying a negative reference.

Aims of a reference

There are two principal aims of a reference:

1. To confirm facts – to confirm the accuracy of the statements made in an application

2. To provide opinions – give the referee's opinion as to the candidate's suitability for the post/course in question, and his/her potential for the future.

The reference relies on both facts and opinions, and these two should be clearly differentiated.

The Reference

1. Be fair to both the student and the recipient of the reference.

2. Ensure the reference is factually accurate and complete. If you need to check information concerning a student contact the Student Centre or School Administration,

3. Make sure your opinions are clearly stated as opinions, are based on fact, and that you are qualified to give such opinions.

4. Do not confuse fact and opinion: "on her performance to date, I would be surprised if X did not get a first class degree" is an opinion, "she will get a first class degree" suggests that the method of classification is beyond doubt.

5. Ensure opinions stated are based on facts known to you, and do not make statements you are not qualified to make. For example, "I consider X to be well suited to the post for which he/she has applied" is preferable to stating "X will be a success in the post of".

6. Particular care should be taken when you are asked for a reference for a student who is not known to you (for example if their supervisor or tutor is absent or has left the university). You should not give opinions which are not your own, and it is preferable to quote someone who has knowledge of the individual, giving the source of the quotation. Do not make statements you cannot justify, or use ambiguous language.

7. You may be asked to express an opinion on issues where you have limited knowledge, e.g. honesty and integrity. It may be necessary to say, for example, "I know of nothing which would lead me to question's X's honesty".

8. The envelope (or email heading) and all correspondence must be marked 'Private and Confidential' and should including the following statement:

> "*This reference is given to you in strict confidence, without liability on the part of the University or the writer, for the purpose of [insert reason e.g. to assist in the selection to the post of../attend the course on] and may be used only for that purpose. The reference may not be disclosed to third parties who are not involved in [the selection process, etc] without the written consent of the sender*."

NB: This liability clause indicates to the recipient that they rely on the reference at their own risk. However, it will not guarantee protection against an action for libel or negligence.

Oral references

The same guidelines apply to references given orally. If possible avoid giving oral references since the information you give may be amended or distorted according to what the enquirer understood you to say or mean. The person receiving an oral reference is likely to make a note of it, so your reference may be written down but you will not control the manner in which it is expressed.

If you have to give a telephone reference, if possible, ask the enquirer what information they require and then arrange a time to call them back. This will help you to verify the bona fide nature of the caller and will ensure you have had time to prepare your response to avoid unintentionally making incautious statements.

Do not make statements that you would not be willing to make in writing.

Unsolicited references

If you are asked to give a reference for a person who has not, to your knowledge, cited you as a referee you should limit your statement to a confirmation of public facts.

Legal Background

Although there is no legal obligation to provide references, referees are under a legal obligation to use due care when compiling references to ensure that they are based on accurate information. If the subject of the reference is defamed orally or in writing, or suffers a financial loss because the contents of the reference were knowingly untrue and given with malice intended, then a civil action for defamation or malicious falsehood might follow. Liability may also come about through carelessness either as to matters of fact or in the formulation of opinion. If the new employer or the subject of the reference suffers as a result of a negligent misstatement made by the referee then he or she will have grounds to sue the referee for negligence for a civil action in the courts.

These guidelines may be amended at any time in the light of experience or changes to legislation.