

Data Protection Policy and Guidance

Table of Contents

1. Purpose	2
Responsibilities	3
Requests for access to personal data	4
2. Guidance	5
Supplementary Guidance For Academic Staff	5
Supplementary Guidance For Administrators.....	7
Guidance For Managers And Supervisors	9

Policy control

Contact/s	Registrar	
Approved at/by	VCEG	
History/Revision dates	Revisions November 2004, July 2007, August 2008, October 2010, July 2017, May 2018	
Audience	Internal (Intranet only)	x
	External (Internet)	x

1. Purpose

1. The University is bound by the Data Protection Act 2018, the General Data Protection Regulations (GDPR) and any arising legislation to register all activities which require the collection, storage, processing, retrieval and disposal of personal data with the Information Commissioner and to undertake these activities in accordance with the provisions of the Act. The Act covers data which is held in a form where it can be processed both automatically on computers and in structured manual filing systems.
2. The activities which the University has registered with the Information Commissioner are:
 - a. Staff, agent and contractor administration
 - b. Advertising, marketing, public relations and general advice services
 - c. Accounts and records
 - d. Education
 - e. Student and staff support services
 - f. Research
 - g. Other commercial services
 - h. Publication of the University magazine
 - i. Crime prevention and the prosecution of offenders
 - j. Alumni relations

A full copy of the University's registration document can be viewed on the Information Commissioner's web-site at: <http://www.ico.gov.uk>. A printed copy may be obtained from the legal office or the University's Data Protection Officer.

3. Personal data is information about any living identifiable individuals, including both statements of fact and expressions of opinion.
4. It is the University's policy to seek consent from individuals for the storage and processing of personal data concerning them, although the University may process personal data without a person's consent where this is permissible under the 2018 Act or the GDPR (for example in pursuit of a contract between the University and an individual). The University will declare the purposes for which personal data will be used and seek specific consent for the disclosure of personal information to third parties, except where this is permissible under the Act and GDPR regulations.
5. Sensitive data include personal data which comprises information on the racial or ethnic origin of an individual, his or her religious beliefs, political opinions or trade union membership, physical or mental health, sexual life, or criminal record or any criminal proceedings or allegations.
6. It is the University's policy to seek explicit consent for the processing and disclosure of sensitive data, and to declare the purposes for which such data may be used.
7. In respect of both personal and sensitive data, the University will:
 - a. use it only for the purposes for which it was obtained;
 - b. collect only that which is necessary in relation to the purpose for which it is required;
 - c. ensure its accuracy and take all reasonable steps to ensure that it is kept up to date;
 - d. retain it only as long as it is needed for the purpose for which it was obtained;

- e. take technical and organisational measures to ensure its security, that no unauthorised or unauthorised processing takes place, and that it is protected against accidental loss, damage or destruction;
- f. ensure that it is not transferred outside the European Economic Area without ensuring that the person's rights and freedoms are adequately protected in the country to which it is transferred.

Responsibilities

8. The University's Data Protection Officer is responsible for maintaining the University's registration with the Information Commissioner, providing guidance and specific advice to staff on data protection issues and their own responsibilities within this policy. Together with the Senior Legal Officer they may authorise the disclosure of personal data to third parties, such as the police and security services, without a person's consent where this is permissible under the GDPR and 2018 Act.

The Registrar's office is also responsible for:

- a. managing relationships with providers of off-site storage and ensuring, as far as is reasonably possible, that the providers' practises fully comply with data protection legislation;
 - b. including specific reference to our requirement that the UK Data Protection Act is followed in contracts with overseas partner organisations;
 - c. publishing and maintaining a retention schedule, setting out the length of time that any personal information should be kept for.
9. The Deputy Vice Chancellor (Academic) is responsible for ensuring that personal data used for research purposes is processed lawfully, taking into account the exemptions contained in Sch 2, Part 6, para 27 of the 2018 Act
 10. The Registrar is responsible for ensuring that personal data used in undergraduate and postgraduate study and dissertations is processed lawfully in accordance with the terms of the Act.
 11. The Chief Information Officer is responsible for ensuring that an adequate framework is in place to enable IT staff to maintain the security of automated storage of centrally held personal data, including password and access controls, system security, back-up procedures, disaster recovery procedures, and secure means for the destruction of such data. He or she is also responsible for ensuring that contractors working on University systems operate within appropriate data security guidelines.
 12. ISD will provide guidance to staff on maintaining the security of data held on local devices, including local PC drives, laptops, disks or other portable devices, but the responsibility for this security and secure destruction of the data remains with the user.
 13. The Director of Facilities and Estates is responsible for ensuring that suitable physical security is available for personal data which is held in accordance with University policy in structured filing systems, including advising on the availability of lockable rooms and key pad entry systems.
 14. Individual staff members and students are responsible for complying with the policy set out in paragraphs 1-7 above, and with any guidance which may be issued by the

Data Protection Officer or the individuals named in paragraphs 8, 9,10, 11 and 12. In particular they are responsible for:

- a. ensuring that the collection and processing of data falls within the purposes declared to the Information Commissioner listed in paragraph 2, and seeking advice from the Data Protection Officer where any uncertainty exists about whether this is the case;
- b. ensuring that personal data about any individual is not passed to third parties without the specific consent of that individual, and that personal references are made within the guidelines laid down by the University;
- c. informing the Data Protection Officer of requests from third parties claiming exemption under the GDPR and 2018 Act, including the police and security services;
- d. ensuring that sensitive personal data is used only for the purposes for which it was collected, and disclosed only to authorised members of the University staff;
- e. ensuring that the data they hold is accurate and up to date;
- f. ensuring the safe-keeping of personal data by not permitting unauthorised access to the data (e.g. ensuring that screens showing personal data cannot be viewed by unauthorised individuals);
- g. the secure disposal of any records containing personal data in line with the University's retention schedule (available through the Registrar's office);
- h. ensuring that those with whom the University contracts have in place suitable arrangements for complying with the Act;
- i. seeking the advice of the Data Protection Officer where they have any doubts in relation to data protection issues.

Requests for access to personal data

15. All individuals about whom the University holds personal data have the right to view the data and any processed data concerning them which is held on automated systems or in structured manual files. Requests to view such data must be made in writing by the individual concerned to the University's Data Protection Officer, stating the nature of the individual's relationship with the institution (such as 'student', 'staff member' etc.)
16. The Legal Office will normally respond to the request within 30 calendar days of receipt of the request provided sufficient information has been provided to identify the individual and locate the information sought. The information provided will be subject to the provisions and safeguards to third parties required in the GDPR and 2018 Act.
17. Standard employment references will be provided by the HR Department on request for ex-employees. Other references, such as those requested by financial institutions, will be provided following authorisation from the current member of staff to release that information.

2. Guidance

UNIVERSITY OF BEDFORDSHIRE DATA PROTECTION: SUPPLEMENTARY GUIDANCE FOR ACADEMIC STAFF

This guidance is intended to cover only the day to day matters you may encounter in relation to data protection, and is by no means exhaustive. Please refer to the [Public Information](#) page and GDPR intranet page for further guidance.

If you require any further advice, please contact the University's Data Protection Officer at DPO@beds.ac.uk for advice whenever you are uncertain of your obligations in respect of data protection.

1. If you keep records of meetings with students, you should inform the student that you are doing so, record only statements of fact, wherever possible, and ensure that you store these records securely and destroy them as soon as they cease to be current.
2. Written comments on assessments, including examination scripts, must be legible and fair. Whilst students do not have the right to view marked formative scripts and assessments under Data Protection legislation, they may ask for an accurate transcript of any comments and remarks to be provided.
3. Do not answer questions from the police, security services or immigration services etc concerning particular students or groups of students, no matter how *bona fide* the enquirer may seem. The enquirer should be referred immediately to the Data Protection Officer.
4. If you are asked for a reference for a student for employment, work placement or education purposes, you should refer to the following document: ['Academic Reference'](#).¹ The Student Information Desk (SID) will provide factual information only for student references; for example course details and content, dates of study, marks obtained, punctuality, attendance etc. If you are asked for a reference for a member of staff for employment purposes, please refer to the Human Resources department.
5. Make sure you destroy any papers containing sensitive information, such as Examination Board papers, securely.
6. Do not disclose details about a student's progress or personal details to anyone except the student concerned. Refer any enquiries from others to your Field Administrator initially.
7. Make sure that students whose undergraduate or Masters dissertations and research activities involve the collection or processing of personal data are aware of the guidance on such issues approved by the Academic Board.
8. Avoid storing personal data on University laptops and do not store personal data outside the University or on home computers. If it is necessary to transport personal data on USB drives, laptops or other portable devices, this data must be encrypted and colleagues take other measures as set out in the IT Data Security Policy, Individual Data Backup policy and any other relevant policies posted on either the Legal Office Data Security or IT policy pages.
9. Do not disclose details concerning a particular student's disability to anyone (including members of staff), unless you are certain that the student has given permission for that person be told of their condition. For further details, see the University's Disability Policy.

¹ https://www.beds.ac.uk/_data/assets/pdf_file/0006/555324/Academic-Reference-letters.pdf

10. Do not pass details of students' names or other details to third parties, such as potential employers etc without first seeking the students' permission.
11. You *can* disclose details of a student's medical history which are known to you if you believe that it is in the student's vital interest (e.g. to a first aider, paramedic or ambulance crew member).

UNIVERSITY OF BEDFORDSHIRE DATA PROTECTION: SUPPLEMENTARY GUIDANCE FOR ADMINISTRATORS

This guidance is intended to cover only the day to day matters you may encounter in relation to data protection, and is by no means exhaustive. Please refer to the [Public Information](#) page and GDPR intranet page for further guidance.

If you require any further advice, please contact the University's Data Protection Officer at DPO@beds.ac.uk for advice whenever you are uncertain of your obligations in respect of data protection.

12. Do not disclose information concerning a student's progress or personal details to anyone except the student concerned, including parents. Some sponsored students grant permission for their sponsor (usually their employer) to receive details on their progress. Check with Faculty Registry Offices if you receive such a request and ensure that the student has given this permission on their registration form.
13. Treat enquiries from Embassies and High Commissions with extreme caution and seek the student's permission before divulging any details, unless the student has consented for the information to be provided on his or her enrolment form.
14. Do not confirm over the telephone that an individual is a student of the University but refer the caller to the Senior Legal Officer.
15. Do not communicate students' results or other details to them over the telephone, without first making absolutely certain that it is the student that you are speaking to. If there is any doubt, a letter providing the requested information should be sent to the address shown on the student record system.
16. Do not answer questions from the police, security services or immigration services etc concerning particular students or groups of students, no matter how *bona fide* the enquirer may seem. The enquirer should be referred immediately to the Senior Legal Officer.
17. Make sure that no unauthorised person can view a student's record inadvertently on your PC screen. Always log out of the student record system or any other system containing personal data (such as the personnel or finance systems) when leaving your machine. Do not leave papers containing personal data visible when you are away from your desk and always lock such material away overnight.
18. Refer specific requests from students to view data concerning them to the Legal Office.
19. Any student can ask to see the comments made about them in Examination Boards or at other meetings. Be sure that all such comments are recorded factually, in minutes with absolutely clarity, with the minimum possible scope for misinterpretation.
20. Do not post students' results on the internet or other non-secure medium and if results are published within the University, ensure that the student's number and not name is used.
21. Do not disclose details concerning a particular student's disability to anyone (including members of staff), unless you are certain that the student has given permission for that person be told of their condition.
22. You must *not* use personal data for a purpose other than that for which it was collected. For example, you cannot use data collected at enrolment to generate alumni lists or

for fundraising activities, or data provided at open days for marketing activities unless specific consent has been given.

23. You *can* disclose details of a student's medical history which are known to you if you believe that it is in the student's vital interest (eg in a medical emergency to a first aider, paramedic or ambulance crew member).

**UNIVERSITY OF BEDFORDSHIRE
DATA PROTECTION: SUPPLEMENTARY GUIDANCE FOR MANAGERS AND
SUPERVISORS**

Recruitment and selection

24. Please note that candidates have a right to see their interview notes. To ensure we comply with all legislative requirements, notes should only address how the candidate fits the selection criteria. Interview notes should be accurate, relevant and objective.
25. We do not need to request information from the second referee of unsuccessful candidates.
26. Applicants' permission should be sought if you intend holding their details for another suitable vacancy in the University.
27. Under no circumstances should information received through an unauthorised channel be considered in making a decision to appoint or reject a candidate. Soliciting for information from an unauthorised third party is strictly prohibited.
28. Requests for access to interview notes should be made to the Legal Office in writing (by email or letter) and a response will be given within 30 calendar days. Please refer any such requests to the Legal Office,
29. All interview notes should be submitted to the Human Resources Department within 48hours of the interview taking place.
30. Whilst it is not always possible for a representative of Human Resources to sit on interview panels, this may be necessary for some senior or internal positions.

Confidentiality

31. Ensure that you keep any records concerning individual staff members (e.g. probationary period reports, career reviews etc.) securely, where colleagues or other unauthorised persons cannot access them. Do not store any details of a sensitive nature concerning staff on your PC where it could be seen by others.
32. Always seek a staff member's permission to inform colleagues of sensitive personal information (e.g. concerning a medical condition or personal problem), and divulge such information only to those who have an immediate need to know. If such information gives you concerns about the safety or security of staff or students, you should discuss the issue with the Human Resources Department.
33. Do not confirm to a telephone enquirer that a particular named individual is a member of the University's staff. Ask for a written request, to make sure the enquiry is from a genuine organisation, and in the meantime seek the individual staff member's permission before giving confirmation.