BISHOP GROSSETESTE UNIVERSITY

Document Administration

Document Title:	Data Protection Policy
Document Category:	Policy
Version Number:	2.1
Status:	Approved
Reason for development:	Scheduled renewal
Scope:	This policy applies to all staff
Author / developer:	Registrar and Secretary
Owner	Registrar and Secretary
Assessment: (where relevant)	Tick relevant assessments / Tick if not applicable ☒ Equality Assessment ☐ Legal ☐ ☒ Information Governance ☐ ☐ Academic Governance ☐
Consultation: (where relevant)	☐ Staff Trade Unions via HR ☐ Students via Bishop Grosseteste University Students' Union ☐ Any relevant external statutory bodies
Authorised by (Board):	Senior Leadership Team & SLT Chair's Action (15.01.16)
Date Authorised:	15.01.2016
Effective from:	January 2016
Review due:	January 2019
Document location:	Website
Document dissemination / communications plan	All staff through Data Protection training (launching Jan/Feb 2016) and via upload to website.
Document control:	All printed versions of this document are classified as uncontrolled. A controlled version is available from SharePoint.

Version 2.1/2015

BISHOP GROSSETESTE UNIVERSITY

DATA PROTECTION POLICY

BISHOP GROSSETESTE UNIVERSITY

1. INTRODUCTION

Bishop Grosseteste University ("the University") needs to retain certain information about its employees, students and other users to allow it to undertake regular monitoring of areas of activity; for example, performance, achievements, and health and safety. It also needs to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government agencies complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the University must comply with the Data Protection Principles, which are set out in the **Data Protection Act 1998** and its subsequent revisions.

In summary, these principles state that personal data shall:

- be fairly and lawfully processed
- be processed for limited purposes
- be adequate, relevant and not excessive
- be accurate and up-to-date
- not be kept for longer than is necessary
- be processed in accordance with the data subject's rights
- be secure
- not be transferred to a country outside the European Economic Area without adequate protection for the individual.

The University and all its staff or others connected with the University who process or use any personal information must ensure that they follow these principles at all times. In addition, they must ensure that the conditions applied by the Act to the processing of personal data are observed so that:

- the individual has given their consent to it being processed
- it is necessary for the performance of a contract with the individual, or
- it is necessary to comply with a legal obligation of the University, or
- it is necessary in order to protect the vital interests of the individual, or
- it is necessary to carry out public functions, or
- it is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual)

Where sensitive data are being processed, strict conditions must be met, which include:

- the individual has given their explicit consent
- it is required by law to process the data for employment purposes
- it is needed in order to protect the vital interests of the data subject or another
- it is necessary to deal with the administration of justice or legal proceedings

In order to ensure that this happens, the University has developed the Data Protection Policy.

BISHOP GROSSETESTE UNIVERSITY

2. STATUS OF THE POLICY

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the University from time to time. Any failures to adhere to the policy may therefore result in the University Disciplinary and Dismissal Policy and Procedures being invoked.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

3. DEFINITIONS

Data

Any information which will either be processed or used on or by a computerised system, or is recorded manually as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

Information covered by the Act could occur in any recorded format including photographs, films, videotapes and audiotapes, images such as those recorded on CCTV, as well as written and electronic records.

Data Controller

A person (individual or body corporate) who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed. For the purposes of this policy, Bishop Grosseteste University is ultimately the Data Controller.

Data Subject

The person about whom the data are held.

Personal Data

Information about a living person who can be identified from those data, or from those data and other information in the possession of, or likely to come into the possession of, the data controller and,

- which is held in a relevant filing system, in an accessible record or computerised record, or on digital, audio or video equipment, and
- which is biographical in a significant sense (mere mention of the data subject in a document does not necessarily amount to personal data), and
- which affects the individual's privacy (whether in his personal or family life, or his business or professional capacity), and
- which has the data subject as its focus rather than some other person with whom he may have been involved

This information is protected by the Act.

A definition of what is meant by a relevant filing system can be found below.

Processing

Covers almost anything which is done with or to the data, including: obtaining data; recording or entering data onto the files; holding data or keeping on file without doing anything to it or with it; organising, altering or adapting data in any way; retrieving, consulting or otherwise using data; disclosing data either by giving it out, by sending it on email or simply by making it available; combining data with other information; erasing or destroying data.

Relevant Filing System

A relevant filing system is a set of records organised by reference to the individual or to their criteria, and structured in such a way as to make specific information readily accessible.

Sensitive Data

The Act introduces categories of sensitive personal data, namely: personal data consisting of information as to an individual's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission by the data subject of any offence; or any [criminal] proceedings or convictions for any offence committed or alleged to have been committed by him.

Notification

The University has a current and up-to-date entry on the Information Commissioner's Register of Data Controllers, which notifies the purposes for which we process personal data. This will be reviewed and renewed on an annual basis.

4. PRINCIPLES

To comply with the Act, the University must follow the eight data protection principles of good information handling. Compliance with the principles is a legal requirement and applies to all personal data for which the University is the data controller. All staff, or any other person the University may have appointed to process personal data on our behalf, must ensure that they follow the data protection principles at all times. This section of the policy contains the key ways in which the University and its staff will work to ensure we follow these principles:

- Whenever we collect personal data, if it is not already clear, we will explain why the data are being collected and what it will be used for. We will also let people know if it is going to pass their data onto other organisations, along with any other details that could help them to understand what we are going to do with their personal data.

- We will only collect and use personal data for specific legitimate purposes, and such data will be kept only for as long as we need it for those purposes. We will not collect excessive or irrelevant information.

- We will only use personal data for the direct promotion or marketing of goods and services with the consent of the data subjects.

- Personal data will be accessible only to those people who need to use such data as part of their work. We will not ordinarily pass personal information to other organisations, unless we have consent or we are legally required to do so.

- We will have appropriate security measures in place to protect personal data, taking account of the nature of the data and the harm that might be caused if data were lost.

- Unauthorised or unlawful accessing, use or disclosure of personal data could lead to disciplinary action, and in some cases may be considered as gross misconduct. In serious cases, it could even be a criminal offence.

- We will provide appropriate training for all relevant staff.

- Data subjects have the right to ask for access to the personal data we hold about them, and are entitled to be given copies of that data. We have procedures in place to allow for this right of access.

- Whenever we propose to transfer personal data outside of the European Economic Area, we will assess the safeguards that are in place.

5. RESPONSIBILITIES

Data Protection Officer

The Registrar and Secretary is currently the University Data Protection Officer. The Registrar and Secretary is responsible for dealing with day-to-day data protection matters and for developing good practice across the University and advising staff on compliance with the Act. The Registrar and Secretary is also the University's primary contact to the Information Commissioner.

Any questions or concerns about the interpretation or operation of this policy should be taken up initially with the Registrar and Secretary.

University Council

The University as a body corporate is the data controller under the Act and the University Council is ultimately responsible for implementing the Data Protection Act 1998 and its subsequent amendments and revisions.

Senior Staff and Line Managers

Senior staff and all in line management roles have the responsibility for ensuring compliance with this policy and for developing and encouraging good practice with regard to handling personal data within their areas. Line managers have the responsibility to promote awareness of the Data Protection Act amongst their staff and advise them to consult with the Registrar and Secretary for advice and guidance when necessary.

Staff and Students are responsible for:

- checking that any information they provide to the University in connection with their employment/registration is accurate and up-to-date
- informing the University of any changes to information which they have provided (e.g. changes of address)
- checking the information that the University will send out from time to time, giving details of information kept and processed about them
- informing the University of any errors or changes
- Staff are responsible for being aware of the Data Protection Act and what it means for the University, in form of this policy.
- Students who intend to use University computer facilities to process personal data must notify, as appropriate, their course tutor, project supervisor or individual supervisor to make sure (before any processing takes place) that any proposed data collection or processing meets the requirements of the Data Protection Act.

The University cannot be held responsible for any errors unless the staff member/student has informed the University of them in writing.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidance for staff (Appendix 1).

6. SUBJECT ACCESS RIGHTS

Staff, students and other users of the University have the right to access any personal data that are being kept about them either on computer or in certain manual records. Any person who wishes to exercise this right should contact the Registrar and Secretary.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing.

The University will normally make a charge of £10 on each occasion that access is requested.

The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days.

7. SUBJECT CONSENT

In many cases, the University can only process personal data with the consent of the individual. In some cases, if the data are sensitive, express written consent must be obtained.

Agreement to the University processing some specified classes of personal data forms a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

Some jobs or courses will bring the applicants into contact with children and/or vulnerable adults, including young people between the ages of 16 and 18. The University College has a duty under the Children Act 2004 and other enactments to ensure that staff are suitable for the job, and that students are suitable for the courses offered. The University also has a duty of care to all staff and students and must therefore make sure that employees and those who use the University facilities do not pose a threat or danger to other users. Please also refer to the University's Code of Practice for Safeguarding Children and Vulnerable Adults.

All students will be required as a condition of their offer to consent to the processing of data required for statistical purposes and also sensitive personal data about themselves as described under the Act. All prospective staff where required by the nature of the post will be asked to complete a Disclosure and Barring Service (DBS) form when an offer of employment is made. All such staff appointments are subject to a satisfactory DBS check being received by the University. More information can be obtained from the Human Resources Department. Similarly, registration on programmes which may involve students in unsupervised access to children will be subject to Disclosure and Barring Service (DBS) checks for which a charge may be made.
Where further data are collected during a member of staff's employments or during a student's studies, they will be informed of this and asked to provide consents where necessary.

8. PROCESSING SENSITIVE INFORMATION

Sometimes it is necessary to process information for instance about a person's criminal convictions, or race and gender and family details. This may be to ensure that the University is a safe place for everyone, or to operate other University policies, such as policies related to the payment of sick pay or matters of diversity and equality. The University may also ask for information about particular health needs, such as allergies to particular forms of medication, or any special needs such as asthma or diabetes or other disabilities. The University will only use the information in the protection of the health and safety of the individual, but will need consent to process the information for example in the event of a medical emergency. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students are asked to give consent for the University to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this without good reason.

9. COLLECTION AND CHECKS

The University will provide opportunities for both staff and students to check and update the personal information held on them by the University. However, staff and students are expected to update their personal data held by the University as soon as such data change.

10. EXAMINATION MARKS

Students will be entitled to information about their marks for both coursework and examinations as part of their tutorial support. This is within the provisions of the Act relating to the release of data. However, this may take longer than other information to provide. The University may withhold awarding a degree in the event that the full course fees have not been paid, or all resources and equipment returned to the University College; in such cases, the University will operate in a

reasonable and proportional manner. The University College may pass on addresses and other contact details to third parties to assist the recovery of such debts.

11. DATA SECURITY

Data should generally be kept in central locations – for example, staff information in Human Resources, student information in the Registry. However, all staff are responsible for ensuring that:

- Any personal data, which they hold, are kept securely, for example:
    - kept in a locked filing cabinet; or
    - in a locked drawer;
    - if computerised, data must be password protected and encrypted if appropriate;
    - for any portable computers or storage devices, guidance on relevant and current measures of information security, password protection or encryption should be obtained from the IT Department;
    - When being processed or accessed, manual records containing personal data should never be left unattended on a desk or in an unlocked room or unlocked filing cabinet (as relevant);
    - Unattended computers containing personal data should be locked to prevent unauthorised access;
    - Personal information must not be disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will normally be considered as a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

12. RETENTION OF DATA

The University will keep some forms of information for longer than others. Details for different types of data and various types of documentation are available in the University's Records Management Policy and related guidance documentation.

13. PUBLICATION OF INFORMATION

The University places certain personal data it holds within the public domain. Personal data in the public domain are data which are publicly available and may be disclosed to third parties without recourse to the individual. Information in the public domain is for instance outlined in the University's Publication Schedule, produced under the requirements of the Freedom of Information Act 2000 and located on the University's website.

The University may not always seek the consent of data subjects when processing personal data, for example, when processing for normal business purposes or when the information is already in the public domain. Where information is placed in the public domain, individuals must be given the opportunity to withhold their consent. It should be noted, however, that many types of information will normally be deemed to be information in the public domain. Any individual who has good reason for wishing particular information to remain confidential should contact the University Registrar and Secretary.

Web authors should note that any personal data accessible from a web page are fundamentally insecure and the type of personal data put on Web pages should reflect this. The University will

normally make staff contact details and other relevant information accessible via the University website following with their consent. If these data are related to a particular responsibility, it will be made clear that such details are in the public domain.

Student data will be made available to relevant staff via University IT systems but access will be restricted by password and governed by the University's IT Systems Security Policy and related guidance.

Personal data which are collected by the University but which are not in the public domain will remain private between the University and the data subject unless one or more of the conditions for processing as specified in the Act applies.

14. REFERENCES

There is no general exemption from the right of subject access for references. There is, however, a special exemption from the right of access to a confidential reference when in the hands of the organisation which gave it. This exemption does not apply once the reference is in the hands of the person or organisation to whom the reference has been given. The recipient is, though, entitled to take steps to withhold information that reveals the identity of other individuals such as the author of the reference.

Confidential references received from third parties shall not therefore be disclosed to data subjects unless the express (written) permission of the writer has been sought and given. Any such subject access requests should be referred to the Data Protection Officer.

<u>Writing references:</u>

Verbal or telephone references should be avoided for both staff and students. A written reference must be provided.

In writing any reference, the writer owes a "duty of care" to both the subject and the recipient. When writing a reference it must be headed "Confidential – for the attention of the addressee/committee/panel only" and state that the reference is only given for the benefit of the addressee(s). The University does not normally provide "open references" for staff.

Copies of all references should be placed in the relevant personnel file.

All students can be provided with a University reference which is prepared by relevant academic staff and held in the student's central file.

References are prepared following a standard template. Students have the opportunity to see and comment on accuracy and other matters as relevant to their course.

When writing references for staff or students, the following sentence should be included:
"Although references are given in good faith, I hope that you will understand that the University must record that it accepts no liability, in negligence or otherwise, for the statements or information contained in this reference".

[See the ICO's "Data Protection Good Practice Note: Subject access and employment references"]

BISHOP GROSSETESTE UNIVERSITY

15. CLOSED CIRCUIT TELEVISION (CCTV)

The University College operates a CCTV system which monitors certain areas of the estate. The system has been installed to reduce the fear or likelihood of criminal activities and damage, prevent trespass and unauthorised access, and to provide a greater feeling of safety for students, staff and the general public whilst on University College premises.

Designated operatives include the Head of Estates, Porters, the Maintenance Engineer and the Director of Resources.

The images shown and recorded by the system are kept in accordance with the Data Protection Act 1998. The equipment does not record sound.

16. USING RESOURCES FOR PERSONAL USE

Staff and students may not process or hold personal data on other individuals for any purposes not related to their work. **Any failures to adhere to the policy may therefore result in the University Disciplinary and Dismissal Policy and Procedures being invoked.**

17. RESEARCH

Staff and students may only collect personal data as part of research activity for which they have prior and explicit approval given by the relevant University committee, group or other authority dealing with research ethics. Staff and students who are collecting personal data must abide by this Policy.

The University recognises that good research is underpinned by good research data management. External organisations providing support and funding for research and related activities, including the European Union and Government agencies, will normally have specific requirements for the retention and safeguarding of data. These requirements will be addressed through review prior to acceptance of the requirements of each case, in line with the University's Records Management Policy and related guidelines. In accordance with the recommendations of Research Councils UK, the university expects researchers to:

- keep clear and accurate records of the research procedures followed and the results obtained, including interim results
- hold records securely in paper or electronic form
- make relevant primary data and research evidence accessible to others, as appropriate legally, ethically and as per the funder's data policy, for reasonable periods after the completion of the research; data should normally be preserved and accessible for at least 10 years
- manage data according to the research funder's data policy, best ethical practice and all relevant legislation
- wherever possible and appropriate, deposit data permanently within a national collection

If no appropriate national collection exists then following the completion of the research project all data may be deposited in a secure central storage facility to be provided by the University, as appropriate. In order to meet these expectations, the Principal Investigator is, at an early stage of their research project, encouraged to produce and then follow a data management plan (DMP).

BISHOP GROSSETESTE UNIVERSITY

18. CONCLUSION

Compliance with the Data Protection Act 1998 is the responsibility of all members of the University. Any deliberate breach of this data protection policy may lead to the University College disciplinary and Dismissal Policy and Procedures being invoked, or access to University College facilities being withdrawn, or criminal prosecution. Any queries or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

BISHOP GROSSETESTE UNIVERSITY

Appendix A
DATA PROTECTION ACT 1998

Note that details of the Data Protection Act and the Schedules can be found at:
http://www.legislation.gov.uk/ukpga/1998/29

Staff Guidelines

1. Staff will process personal data on a regular basis. The University will ensure that staff and students give their consent to processing and are notified of the categories of processing, as required by the Act.
2. Information about an individual's physical or mental health or condition; sexual life; religious views; ethnicity or race; or other specific characteristics as listed in the Equality Act 2010 is sensitive and can only be collected and processed with their express consent.
3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the University's Data Protection Policy. In particular, staff must ensure that records are:
    - accurate;
    - up-to-date;
    - fair;
    - kept and disposed of safely, and in accordance with the University's policies on Data Protection and Records Management.
4. Individual members of staff are responsible for ensuring that all data they are holding are kept securely.
5. Staff must not disclose personal data, unless for normal academic, administrative or pastoral purposes, without authorisation or agreement from the data controller, or in line with the University's policy. For instance, information on students must not be given to third parties (such as parents or future employers) other than by (written and signed) permission from the students themselves.
6. Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording 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 individual or data subject been told that this type of data will be processed?
- Are you authorised to collect/store/process/disclose 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 the best interests of the student or the staff member to collect and retain the data?
- Have you notified the Registrar and Secretary that you intend to hold the data?
- How long do you need to keep the data for, and what is the mechanism for review/destruction?