BISHOP GROSSETESTE UNIVERSITY

BISHOP GROSSETESTE UNIVERSITY DATA PROTECTION POLICY

1. INTRODUCTION

Bishop Grosseteste University ("the University") needs to retain certain information about its employees, students and other users to enable 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 or body unlawfully. To do this, the University must comply with data protection regulations (in particular the European General Data Protection Regulation [GDPR], see https://www.eugdpr.org/eugdpr.org.html) and relevant UK legislation.

In order to ensure that this happens, the University has developed this Data Protection Policy. It should be read in conjunction with the University's Data Breach Policy and Privacy Policy.

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 Policy, Procedure and Guidance being invoked.

This policy applies to all parties acting on behalf of the University. The provisions are intended to protect the personal data of students and the public.

3. DEFINITIONS

A glossary of term used in the EUGDPR can be found at: https://www.eugdpr.org/glossary-of-terms.html .

In particular, the following definitions, as given on the Information Commissioner's Office website, (www.ico.org.uk) should be noted:

Data Controller	"A controller determines the purposes and means of processing personal data." The University acts as the data controller for data it collects.
Data Processor	"A processor is responsible for processing personal data on behalf of a controller." The University may process data for external organisations.
Data Subject	"A natural person whose personal data is processed by a controller or processor." (EUGDPR)
Personal data	"The GDPR applies to 'personal data', meaning any information relating to an identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal

	data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual."
Sensitive personal data/ special categories of personal data	"The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10 of the GDPR)".

4. PRINCIPLES

In accordance with the GDPR, personal data shall be:

a) "processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

The University and all its staff or others connected with the University who process or use any personal information must ensure that they the above at all times. In addition, it must ensure that the processing of data is undertaken under 1 or more of the following conditions:

a) Consent: the individual has given clear consent for the University to process their personal data for a specific purpose.
b) Contract: the processing is necessary for a contract the University has with the individual, or because the individual has have asked the University to take specific steps before

entering into a contract.

c) Legal obligation: the processing is necessary for the University to comply with the law (not including contractual obligations).
d) Vital interests: the processing is necessary to protect someone's life. Processing of personal data based on someone's vital interest should, in principle, take place only where the processing cannot be based on another legal basis, and where the individual is incapable of giving consent.
e) Public task: the processing is necessary for the University to perform a task in the public interest or for its official functions and the task or function has a clear basis in law.
f) Legitimate interests: the processing is necessary for the legitimate interests of the University or the legitimate interests of a third party. Please note: this interest may be overridden by the interests or fundamental rights of the data subject and cannot be used by a public authority processing data to perform official tasks.

The University may need to process special categories of personal data. A definition of such data is included in section 3 above. The University will determine the relevant condition for processing special category data and document it. The University acknowledges that children (under the age of 13) cannot give consent without parental or guardian involvement. (This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval.)

The University and its staff ('we') will work to ensure that:

a) Whenever we collect personal data, we will ensure transparency at the point of data collection (see the University's Data Privacy Policy). If it is not already clear, we will explain why the data is being collected and what it will be used for. We will also let people know we are 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.
b) We will only collect and use personal data for specific legitimate purposes (see above), 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.
c) We will only use personal data for the direct promotion or marketing of goods and services with the consent of the data subjects.
d) 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.
e) 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.
f) 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.
g) We will provide appropriate training for all staff.
h) We will acknowledge the rights of the Data Subject under the GDPR and relevant UK legislation and will ensure that there are clear procedures in place should a data subject wish to enact these rights.
i) We will implement appropriate technical and organisational measures to ensure, and be able to demonstrate, that processing of data (including by external data processors) is performed in such a way as to take into account the rights and freedoms of natural persons. This will be undertaken in proportion to the processing activities being undertaken.
j) We will seek to implement a culture of Privacy by default and Privacy by design in all data

processing activities, including the use of Data Privacy Impact Assessments where the processing is "likely to result in a high risk to the rights and freedoms of natural persons".

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

5. RESPONSIBILITIES

University Council

The University as a body corporate is the data controller under the Act and University Council is ultimately responsible for implementing data protection regulations and UK legislation.

Chief Operating Officer

The Chief Operating Officer holds accountability for the operation of this policy.

Data Protection Officer

The Registrar is currently the University Data Protection Officer. The Registrar will act independently to:

a) inform and advise the University and its employees of their data protection obligations under the GDPR ;
b) monitor the University's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits;
c) advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes;
d) serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting;
e) Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

The Registrar will be assisted in these duties by the Directors of the University. Any questions or concerns about the interpretation or operation of this policy should be taken up initially with the Registrar.

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 GDPR and relevant UK legislation amongst their staff and advise them to consult with the Chief Operating Officer, Registrar or Governance Team for advice and guidance when necessary.

Staff and Students, as Data Stewards of the data in their care, are responsible for:

a) checking that any information they provide to the University in connection with their employment/registration is accurate and up-to-date;

b) informing the University of any changes to information which they have provided (e.g. changes of address);
c) checking the information that the University will send out from time to time, giving details of information kept and processed about them;
d) informing the University of any errors or changes;
e) Staff are responsible for being aware of the GDPR and relevant UK legislation and what it means for the University, in form of this policy;
f) 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 GDPR and relevant UK legislation.

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 from third parties (e.g. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with this policy and relevant training and guidance provided by the University.

6. Personal Privacy Rights

Rights for individuals under the GDPR include:
a) subject access ;
b) to have inaccuracies corrected;
c) to have information erased;
d) to object to direct marketing;
e) to restrict the processing of their information, including automated decision-making;
f) data portability.

People for whom the University holds and processes personal data have the right to confirmation that their data is being processed and 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 their personal privacy rights should follow the procedures outlined at http://www.bishopg.ac.uk/about/Governance/policies-procedures/ .

The University aims to comply with these requests for access to personal information as quickly as possible, but will ensure that it is provided within 1 calendar month.

7. LAWFUL PROCESSING

The lawful basis under which data is processed by the University is laid out in the University's Information Asset Register. This includes any relevant special category and criminal offence data conviction condition. (See also the University's Privacy Policy at: http://www.bishopg.ac.uk/about/Governance/policies-procedures/)

Some jobs or courses will bring the applicants into contact with children and/or at-risk adults,

including young people between the ages of 16 and 18. The University has a duty to ensure that staff are suitable for their job, and that students are suitable for the courses offered to them. The University also has a duty of care to all staff and students; therefore it must take reasonable steps to ensure 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.

Relevant 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 People and Organisational Directorate. Similarly, registration on programmes which may involve students in unsupervised access to children and or at-risk adults will be subject to Disclosure and Barring Service (DBS) checks for which a charge may be made. Where further data is collected during a member of staff's employments or during a student's studies, they will be informed of this, the lawful purpose for processing and asked to provide consents where necessary.

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/others. Offers of employment or programme places may be withdrawn if an individual refuses to consent to this without good reason.

8. 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.

9. 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.

10. 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.

11. 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, however, it will always have a lawful reason for processing. 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 Registrar (via regulatorycompliance@bishopg.ac.uk).

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 university contact details and other relevant work related information accessible via the University's website with their consent.

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.

12. USING RESOURCES FOR PERSONAL USE

Staff and students may not access, 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.**

BISHOP GROSSETESTE UNIVERSITY

13. 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:

a) keep clear and accurate records of the research procedures followed and the results obtained, including interim results;
b) hold records securely in paper or electronic form;
c) 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;
d) manage data according to the research funder's data policy, best ethical practice and all relevant legislation;
e) 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).

14. COMPLAINTS

Any person, who considers that the policy has not been followed in respect of personal data about themselves, should initially raise the matter with the governance team (regulatorycompliance@bishopg.ac.uk), unless they believe that the governance team have not followed policy, in which case the Director of IT and Systems (barry.clarkson@bishopg.ac.uk) should be contacted.

If the matter is not resolved it should be raised as a formal complaint using the University's complaint procedures available at http://www.bishopg.ac.uk/about/governance/policies-procedures/ .

15. CONCLUSION

Compliance with the GDPR and relevant UK legislation is the responsibility of all members of the University. Any deliberate breach of this data protection policy may lead to the University's disciplinary and Dismissal Policy and Procedures being invoked, or access to University's facilities being withdrawn, or criminal prosecution.

16. LINKED POLICIES

Bishop Grosseteste University's:

- Data Breach Policy
- Privacy Policy
- Records Management Policy
- IT Systems Acceptable Use Policy
- CCTV Policy
- Whistleblowing Policy
- Student advice confidentiality policy

The above policies are available at **http://www.bishopg.ac.uk/about/Governance/policies-procedures/** .

Relevant staff policies are available through SharePoint

17. FURTHER INFORMATION

Further Information on this Policy can be obtained from the Registrar via email: Regulatorycompliance@bishopg.ac.uk or in writing to Regulatory Compliance, Bishop Grosseteste University, Longdales Rd, Lincoln. LN1 3DY.