BISHOP GROSSETESTE UNIVERSITY

Document Administration

Document Title:	Data Protection Policy
Document Category:	Policy
Version Number:	2.0
Status:	APPROVED
Reason for development:	This policy outlines the University's commitment to protecting individuals' rights to privacy in accordance with the Data Protection Act 2018 (including any replacement of that Act) incorporating the UK General Data Protection Regulation.
Scope:	All staff
Developer and Owner:	Director of CIS, Strategy & Performance
Assessment: (where relevant)	Tick relevant assessments ☒ 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):	University Council
Date First Authorised:	15 January 2016
Reviewed and Effective From:	February 2025
Review due:	June 2028 – unless required earlier
Document location:	University Website
Document control:	All printed versions of this document are classified as uncontrolled. A controlled version is available from the University Website.
Alternative format	If you require this document in an alternative format, please contact policy@bishopg.ac.uk

Please note this document remains valid until formally revoked or replaced by the University.

Version Control Table

Version Number	Date Authorised	Summary of key changes
1.0	15 January 2016	Policy first issued and approved by University Council.
2.0	18 February 2025	A full review and revised to align with current practices and ICO guidelines and regulations.

BISHOP GROSSETESTE UNIVERSITY

DATA PROTECTION POLICY

1. INTRODUCTION

1.1. Bishop Grosseteste University ("the University") is committed to a policy of protecting individuals' right to privacy in accordance with the Data Protection Act 2018 (including any replacement of that Act) (the "DPA") incorporating the UK General Data Protection Regulation (the "GDPR", together, the "Data Protection Laws"). This policy sets out that commitment. The University recognises that correct and lawful treatment of Personal Data contributes to the good reputation of the University by demonstrating its integrity and its respect for those it deals with. The University needs to Process certain information about its staff, students, and other individuals it has dealings with. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

1.2. In order to ensure that this happens, the University has developed the Data & Information (Records) Management Framework to oversee data governance.

2. BACKGROUND

2.1. The purpose of the Data Protection Laws is to protect the rights and privacy of living individuals and to ensure that Personal Data is Processed fairly and transparently.

2.2. The University collects, holds, and uses Personal Data relating to individuals who have/have had a relationship with the University. The purpose of this policy is to ensure that the University:

2.2.1. operates procedures and practices that conform to the requirements of the Data Protection Laws when working with Personal Data;

2.2.2. clearly defines responsibilities and accountability for data protection;

2.2.3. provides staff, researchers and students with the resources, knowledge, competencies, and procedures to work with Personal Data in compliance with the Data Protection Laws and with this policy.

3. POLICY STATEMENT

3.1. This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that employees will familiarise themselves with and act in accordance with this policy. The University may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be managed in accordance with the University's policy framework.

3.2. Any failure to follow this policy by staff or students may result in disciplinary action. Any failure by affiliates to follow this policy may result in their access to University IT systems and premises being restricted or removed.

4. DEFINITIONS

4.1. This policy tries as far as possible to avoid using technical terms. However, there are some terms used in the Data Protection Laws that it is helpful to have an understanding of in the context of data protection compliance. To assist such understanding, we have set out a list of key terms and their meanings below. Where these terms are used in this policy, they should be read and applied in this context.

4.2. 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. The University may also engage third party organisations (data processors) to provide services on its behalf
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)".

5. PRINCIPLES

5.1. In accordance with the GDPR, personal data shall:

5.1.1. Be processed lawfully, fairly, and transparently. This means that those responsible for Processing Personal Data must make reasonable efforts to ensure that Data Subjects are informed of the identity of the Data Controller (i.e. the University), the purpose and legal basis of the Processing, any disclosures to third parties that are envisaged and an indication of the period for which the Personal Data will be kept.

5.1.2. Only be processed for specified and lawful purposes.

5.1.3. Only be held that is relevant and accurate, and where practical, we will keep it up to date. This means information that is not strictly necessary for the purpose for which it is obtained should not be collected. If Personal Data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed. Our Privacy Policy outlines what we collect, and how we use it.

5.1.4. Not kept for longer than is necessary.

5.1.5. Be kept secure and employ a "data protection by design" approach to systems engineering and projects that promotes and incorporates privacy and data protection considerations from the outset.

5.1.6. Only be shared where we have appropriate data sharing agreements in place with third parties.

5.1.7. Not be transferred to countries outside of the European Economic Area (EEA) without adequate protection.

5.2. In addition to 5.1, The University will endeavour to;

5.2.1. Review our range of governance and privacy policies to ensure they are kept up to date.

5.2.2. Undertake training and awareness raising activities for staff and students so that they understand their obligations.

5.2.3. Only work with companies for data processing services that are data protection compliant, and which enter into appropriate data processing agreements

5.3. The University and all its staff or others connected with the University who process or use any personal information must ensure they observe the above principles at all times.

5.4. It is the responsibility of all individual staff, students, and other persons to ensure that Personal Data held by the University is accurate and up to date. Completion by a Data Subject of an appropriate registration or application form, etc. will be taken as an indication that the data contained therein is accurate. Individuals should notify the University of any changes in circumstance to enable personal records to be updated accordingly. Students should use "Student Gateway" or contact the Faculty Administration Office (fao@bishopg.ac.uk) (applicants should contact the Student Admissions Team admissions@bishopg.ac.uk). Staff should contact the Human Resources (hrhelp@bishopg.ac.uk) or update their personal details using self service via MyDay. It is the responsibility of the University to ensure that any notification regarding change of circumstances is noted and acted upon.

5.5. In addition, it must ensure that the processing of data is undertaken under one or more of the following conditions:

5.5.1. Consent: the individual has given clear consent for the University to process their personal data for a specific purpose.

5.5.2. Contract: the processing is necessary for a contract the University has with the individual, or because the individual has asked the University to take specific steps before entering into a contract.

5.5.3. Legal obligation: the processing is necessary for the University to comply with the law (not including contractual obligations).

5.5.4. 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.

5.5.5. 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.

5.5.6. 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.

5.6. 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. Further information is provided on the processing of personal data, outlined within the Privacy Policy.

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

5.7.1. the University will publish privacy notices in respect of its Processing of Personal Data of students, staff, alumni, certain partners and visitors, which tell those people what data is collected about them, what it is used for, the legal basis for Processing the data, who it will be shared with and how long it will be held for. When gathering Personal Data or establishing new data protection activities, members of staff should check existing privacy notices to see whether they need to be updated to reflect the new activities, or whether new privacy notices are required to cover that activity. They should also ensure that any new Processing activities are added to the University's Record of Processing Activities, which operates as a Data Asset Register, whenever we collect personal data, we will ensure transparency at the point of collection.

5.7.2. 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.

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

5.7.4. 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.

5.8. 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.

5.8.1. 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.

5.8.2. We will provide appropriate training for all staff.

5.8.3. 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.

5.8.4. 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.

5.8.5. 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."

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

6. RESPONSIBILITIES

6.1. University Council

6.1.1. 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.

6.2. Deputy Vice Chancellor (Operations)

6.2.1. The Deputy Vice Chancellor (Operations) holds accountability for the operation of this policy on behalf of the University Executive Group.

6.2.2. The Deputy Vice Chancellor (Operations) has delegated responsibility for day-to-day data protection matters to the Director for Corporate Information Systems, Strategy & Performance, who has been appointed as the Data Protection Officer for the University.

6.3. Data Protection Officer (DPO)

6.3.1. The Director for Corporate Information Systems, Strategy & Performance is currently the University Data Protection Officer. They act independently to:

6.3.1.1. inform and advise the University and its employees of their data protection obligations under the GDPR ;

6.3.1.2. 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;

6.3.1.3. advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes;

6.3.1.4. serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting; and

6.3.1.5. serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

6.3.2. The Director for Corporate Information Systems, Strategy & Performance or other delegated senior member of the Information Compliance Team will operate as Chair of the established Data Governance Group which has been established to define, approve, steer and monitor Information Management and Governance (including in relation to data protection) within the University. This includes overseeing information governance roles and responsibilities, policies and procedures and activities in order to embed compliance, promote best practice, and provide technical solutions to all staff across the University, ensuring the development and delivery of the University's Data Strategy.

6.4. **Senior Leadership Team (SLT) & Senior Management Group (SMG) members**

6.4.1. Senior Leadership Team (SLT) & Senior Management Group (SMG) members are responsible for ensuring that staff in their area are aware of this policy and their responsibilities.

6.4.2. SLT and SMG members are expected to encourage and promote a culture of good records and information/data management within their area of responsibility.

6.4.3. 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 for advice and guidance when necessary.

6.5. **All staff are responsible for:**

6.5.1. ensuring that they have undertaken University-provided data protection training;

6.5.2. checking that any information that they provide the University in connection with their employment is accurate and up to date and for informing the University of any changes to their personal data (e.g., change of address);

6.5.3. ensuring that any Personal Data Processed by them is Processed in accordance with the Data Protection Laws and with this policy;

6.5.4. Staff who have a responsibility for supervising/mentoring students who are undertaking Processing of Personal Data (e.g. as part of a research project or on a placement) have a responsibility to ensure that the student is informed as to their responsibilities under the Data Protection Laws, by reference to this policy and other relevant materials;

6.5.5. All students are responsible for checking that any information that they provide the University in connection with their enrolment and study at the University is accurate and up to date and for informing the University of any changes to their Personal Data (e.g., change of address); and

6.5.6. Students who are considering Processing Personal Data as part of their studies must notify and seek approval relevant research ethics approvals process. Such students will be bound by the Data Protection Laws and by this policy and must ensure that they act in accordance with both.

7. Subject Data Rights

7.1. Under the Data Protection Laws, Data Subjects have the following rights regarding the Processing of their Personal Data and the data that are recorded about them:

7.1.1. subject access ;

7.1.2. to have inaccuracies corrected;

7.1.3. to have information erased;

7.1.4. to object to direct marketing;

7.1.5. to restrict the processing of their information, including automated decision-making; and

7.1.6. data portability.

7.2. To access personal data held by the University about them (please see Rights of Access to Personal Data); to require the University to rectify any inaccurate personal data held by it about them; and to require the University to erase personal data held by it about them. This right of erasure will only apply where, for example, the University no longer needs to use the Personal Data to achieve the purpose it was collected for; or where the Data Subject withdraws their consent if the University is using their Personal Data based on Data Subject consent; or where the Data Subject objects to the way the University Processes their data and this is upheld.

7.3. To restrict the University's Processing of the Personal Data it holds about them. This right will only apply where, for example, the Data Subject disputes the accuracy of the Personal Data the University holds; or where they would have the right to require the University to erase the Personal Data but would prefer that its Processing is restricted instead; or where the University no longer needs to use the Personal Data to achieve the purpose for which it was collected, but it requires the data for the purposes of dealing with legal claims. In cases where the University has disclosed data to another party, and it is not disproportionate for the University to do so, it will let the recipients of the data know that the University has rectified, erased, or restricted the Processing of it.

7.4. To receive personal data, which they have provided to the University, in a structured, commonly used, and machine-readable format (where Processing is automated and is either based on consent or is necessary for the performance of a contract). Data Subjects also have the right to transfer (or require the University to transfer) this Personal Data to another organisation (for example, a new employer or higher education institution).

7.5. To object to the University's Processing of Personal Data it holds about them (where its justification for Processing the data is either that the Processing is necessary for the performance of a task in the public interest, or for the purposes of its own legitimate interests).

7.6. To require a review. Data Subjects may ask the University to review any decisions that it has made about them using automated Processing.

7.7. To withdraw their consent, where the University is relying on it to Process their personal data.

7.8. To prevent Processing for the purposes of direct marketing.

7.9. The University will have procedures in place to ensure that these rights can be exercised and will publicise these on its website.

7.10. If staff or students have concerns about the way in which their personal data is being used or Processed by the University, they may contact the Data Protection Officer, in the first instance. If after this, they are not satisfied by the University's response they have the right to lodge a formal complaint with the Information Commissioner's Office.

8. Special Categories of Personal Data

8.1. Special Categories of Personal Data are afforded a higher level of protection by law. It will normally be necessary to have an individual's explicit consent to Process Special Categories of Personal Data, unless exceptional circumstances apply or the Processing is necessary to comply with a legal requirement, including to fulfil its employment duties as an employer. The consent should be a freely given (i.e. it should not be conditional), specific (i.e. it should set out exactly what is being consented to), informed, (i.e. it needs to identify the relevant data, why it is being Processed and to whom it will be disclosed) and an unambiguous indication of the individual's wishes by which they, by a statement or by a clear affirmative action (i.e. the ticking of an unticked box) signify their agreement. When relying on explicit consent as the legal basis for Processing Personal Data, there will be instructions with details of how to withdraw their consent, if they wish to do so. Staff should contact the Data Protection Officer for more information about the conditions to be satisfied to enable Processing of Special Category Personal Data.

9. Rights of Access to Personal Data

9.1. As set out in the Privacy Policy, individuals have the right (subject to certain exceptions) to request access in relation to information held by the University about them in electronic format and/or in manual records which form part of a relevant filing system, save where exemptions apply. A request of this nature is known as a "subject access request". All such requests should be referred immediately to the Corporate Information Team, via a Helpdesk submission on the Staff Portal, alternatively by emailing informationcompliance@bishopg.ac.uk.

9.2. The University is required to respond to requests without delay and in any event within one month of their receipt.

9.3. Where a request is made for examination scripts (where these are still held), no copies of the scripts will be provided but students may view the script in the presence of a representative from Faculty Administration Office team. Examiners' comments can be transcribed and provided as part of a subject access request.

9.4. In order to respond efficiently to data subject rights requests the University needs to have in place appropriate records management practices. See the Data & Information (Records) Management Policy for further information on records management.

9.5. In addition to the above, where the University is acting as a Data Processor, it will have a responsibility to aid the third party it is Processing Personal Data on behalf of, in respect of individuals exercising their rights. The contract between the University and the third party it is Processing Personal Data on behalf of, may also have additional contractual restrictions or timescales in respect of such support/ assistance. Checks will be required to be made as to the contractual position carefully prior to (a) responding to a request made directly by an individual or third party, or (b) providing assistance to the third party.

10. DISCLOSURE OF PERSONAL DATA

10.1. The University must ensure that Personal Data is not disclosed to unauthorised third parties. This includes family members, friends, government bodies, the media, and in certain circumstances, the Police.

10.2. All staff and students should exercise caution when asked to disclose Personal Data held by the University about another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's personal details to someone who wished to contact them regarding a non-work-related matter, especially when such details are not otherwise publicly available (such as work contact details on the University website). The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of university business.

10.3. This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

10.3.1. where the disclosure is in the legitimate interests of the University (e.g., disclosure to staff – Personal Data can be disclosed to other University employees if it is clear that those members of staff require the information to enable them to perform their jobs);

10.3.2. where the University is legally obliged to disclose the data (e.g., HESA and HESES returns, ethnic minority and disability monitoring, all of which are covered in the University's privacy notices for staff and students); or

10.3.3. where disclosure of data is required for the performance of a contract (e.g., informing Student Finance England or a sponsor of course changes/withdrawal, etc.).

10.4. If Personal Data is to be shared with a third party in connection with the performance of a contract, then approved data protection clauses must be included in the relevant contract. The University Data Protection Officer should be consulted on every occasion before any such contracts are entered into and Personal Data must not be shared with the third party until an appropriate contract is in place.

10.5. The Data Protection Laws permit certain disclosures without notification to the Data Subject in certain cases, so long as the information is requested for one or more of the following purposes:

- to safeguard national security**
- prevention or detection of crime including the apprehension or prosecution of offenders**;
- assessment or collection of tax duty**;
- discharge of regulatory functions (includes health, safety, and welfare of persons at work)**;
- to prevent serious harm to a third party; or
- to protect the vital interests of the individual; this refers to life and death situations.

***** Requests must be supported by appropriate paperwork and should follow the agreed protocols if in place. Where a third party request is received citing one of these grounds, the request should be passed to an authorised person within the University for approval before any information is related. The authorised personnel are, the Data Protection Officer or the Deputy Vice Chancellor.***

10.6. If members of staff receive enquiries as to whether a named individual is a member of the University (staff or student), the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e., consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the University may constitute an unauthorised disclosure of Personal Data.

10.7. Unless the Data Subject has requested otherwise, Personal Data should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request, sent via email to informationcompliance@bishopg.ac.uk. Ideally a statement from the Data Subject consenting to disclosure to the third party should accompany the request.

10.8. As an alternative to disclosing Personal Data, the University may offer to do one of the following:

- pass a message to the Data Subject asking them to contact the enquirer; or
- accept a sealed envelope/incoming email message and attempt to forward it to the Data Subject.

10.9. Please remember to inform the enquirer that such action will be taken conditionally: i.e., "if the person is a member of the University" to avoid confirming their membership of their presence in or their absence from the institution.

If in doubt, staff should seek advice from the University Data Protection Officer

11. LAWFUL PROCESSING

11.1. The lawful basis under which data is processed by the University is laid out in the University's Record of Processing Activities. This includes any relevant special category and criminal offence data conviction condition and outlined in the University's Privacy Policy.

11.2. 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 Safeguarding Children and at-risk Adults Policy.

11.3. 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 Human Resources. 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.

11.4. 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.

11.5. 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.

11.6. 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, ensuring effective support and facilities are provided, or to comply with regulatory reporting obligations. Offers of employment or programme places may be withdrawn if an individual refuses to consent to this without good reason.

12. COLLECTION AND CHECKS

12.1. 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.

13. DATA SECURITY

13.1. All staff are responsible for ensuring that any Personal Data (on others) which they hold are kept securely in line with this policy, and others including the University's IT Security Policy and Procedure and in appropriate systems and that such data is not disclosed to any unauthorised third party.

13.2. Data should generally be kept in central locations, and only accessible to those who need it to use it. All staff are responsible for ensuring that:

Any personal data, which BGU hold, is 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);
- care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screensavers and manual records should not be left where they can be accessed by unauthorised individuals;
- personal information must not be disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party;
- where possible, files containing data should be stored via a secure link, and not as an attachment to an email i.e., OneDrive, which enables greater security and control of access internally and externally.

13.3. Personal Data must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, or DVDs) or mobile devices (laptops, tablets, or smart phones) unless it is encrypted or password protected, and the key kept securely. A backup copy should also be kept on the secure University servers. Personal Data must not be stored in generic personal cloud services such as Dropbox or Google etc.

13.4. Care should be taken when sending emails that contain Personal Data, even internally between departments, particularly in the case of Special Category data as this will have restricted access and utilization, defined by the lawful purpose of data collection. Retention and deletion of this data, if accessed as a copy of the master record should be destroyed once the purpose of its use is finalized in order to mitigate any potential breach in the future.

13.5. Staff who are recording student data via their own means i.e., excel documents should seek guidance from the Data Protection Officer in how to effectively store and protect this information, and to understand their accountability and responsibility under GDPR in doing so. For clarity, this is any form of data which identifies a staff or student including registers and attendance records.

13.6. 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.

13.7. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of Personal Data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be securely wiped clean before disposal. If in doubt as to what the correct security measures are for the deletion or disposal of Personal Data, advice should be taken from IT Support via the Staff Portal.

13.8. In the event that the University acts as a Data Processor, processing personal data on behalf of a third party, such third party may require additional security arrangements to be implemented. There are also mandatory legal protections which must be included in any contract, and that needs to be flowed down to any sub-processor used by the University.

13.9. Members of the University should consult with the Data Protection Officer to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement, including cloud-based guidance.

14. INTERNATIONAL TRANSFERS

14.1. Data must not be transferred outside of the European Economic Area (EEA) - the twenty-seven EU Member States together with Iceland, Liechtenstein, and Norway - without the explicit consent of the individual, or unless the Personal Data is adequately protected, or an exemption applies.

14.2. Adequate protection can be provided if:

14.2.1. the data protection arrangements in the destination country have been approved by the ICO (there is a list of approved countries on the ICO website); or

14.2.2. the recipient is a signatory to an ICO approved data protection regime; or

14.2.3. the recipient is bound by a contract that ensures that the Personal Data concerned will be adequately protected (for example, incorporating the Standard Contractual Clauses approved by the ICO).

14.3. Members of the University should be particularly aware of this when contracting with a third party for the Processing of Personal Data (including for IT support, collaborative provision, or research purposes) or when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

14.4. In addition to the above, where the University is acting as a Data Processor, the contract between it and the third party it is Processing Personal Data on behalf of may have additional contractual restrictions in respect of international transfers of such data. Members of the University should check the contractual position carefully prior to transferring the Personal Data and check with the Data Protection Officer if they are unclear how to proceed.

15. REPORTING BREACHES

15.1. All staff, students, contractors, partnerships, suppliers, and governing board members of the University have an obligation to report actual or potential data protection compliance failures to the Data Protection Officer immediately they become aware of them.

15.2. The Data Protection Laws provide that breaches must be notified to the ICO as soon as possible and in any event within 72 hours of becoming aware of them. Notification to the Data Protection Officer also allows the University to:

15.2.1. investigate the failure and take remedial steps if necessary; and

15.2.2. make any other applicable notifications, including to affected Data Subjects where appropriate.

15.3. University staff may be required as part of their duties to support the University in any such investigation.

15.4. Where the University is acting as a Data Processor, it will have a responsibility to notify actual or potential data protection compliance failures to the third party it is Processing personal data on behalf of. The contract between the University and the third party it is Processing personal data on behalf of may also have additional contractual restrictions or timescales in respect of such support/ assistance. Members of the University should check the contractual position carefully and check with the Data Protection Officer if they are unclear how to proceed.

15.5. The submission of a data breach, or potential breach, is required immediately by the member of staff who identifies it. This can be done by the dedicated self-service form on the Staff Portal or by emailing informationcompliance@bishopg.ac.uk

Upon investigation, if it has been found a member of the University had knowledge of a breach and failed to report, this may result in the University Disciplinary and Dismissal Policy and Procedures being invoked.

For further Guidance, please review the Data Breach Policy or contact informationcompliance@bishopg.ac.uk

16. ACTING AS A DATA PROCESSOR

16.1. When the University Processes the Personal data of students, staff, suppliers, alumni, and other individuals (in a professional or personal context) it is ordinarily the case that the University would be known as a Data Controller. A Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, 'Processed'.

16.2. In some limited circumstances, the University may be a Data Processor; i.e., it is Processing the data on behalf of a third party Data Controller.

16.3. If members of the University are handling Personal Data and are not sure whether the University is acting as a Data Controller or a Data Processor, they should contact the Data Protection Officer in the first instance. It is key to understand the relationship, in order to determine how such personal information should be handled.

16.4. The Data Controller has the majority of the obligations under the Data Protection Laws, e.g., in respect of Data Subject rights and ensuring appropriate consents are obtained or privacy notices are given. However, a Data Processor also has a number of obligations under Data Protection Laws. In most cases, the Processing obligations imposed on the University will be guided by the contract entered into between the University and the third party on whose behalf it is Processing.

17. ACCURACY, ADEQUACY, RELEVANCE AND PROPORTIONALITY

17.1. To comply with the Privacy Policy and relating Data Protection Laws, members of the University should make sure data Processed by them is accurate, adequate, relevant, and proportionate for the purpose for which it was obtained. Personal Data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

17.2. Individuals may ask the University to correct Personal Data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Data Protection Officer.

17.3. Staff and students must ensure that Personal Data held by the University relating to them is accurate and updated as required. If personal details or circumstances change, students should use "Student Gateway" or contact the Faculty Administration Office (fao@bishopg.ac.uk) (applicants should contact the Student Admissions Team (admissions@bishopg.ac.uk). Staff should contact the Human Resources (hrhelp@bishopg.ac.uk) or update their personal details using self service via MyDay.

18. RETENTION AND DISPOSAL OF DATA

18.1. The University will keep some forms of information for longer than others. Details for different types of data and various types of documentation is outlined in the Data & Information (Records) Governance Framework, and corresponding Retention Schedule which outlines the retention and disposal of information.

18.2. The University discourages the retention of Personal Data for longer than it is required. Considerable amounts of data are collected about staff, students, applicants, research subjects, etc. However, once a member of staff or student has left the University or the purpose for which that data was collected has ended, it will not be necessary to retain all the information held on them. Some Personal Data will be kept for longer periods than others. The University's Retention and Disposal Schedule should be followed for the retention and disposal of Personal Data.

18.3. The University aims to reduce the duplication of personal data and will encourage as far as possible the use of definitive central sources of information for data used across the University. Where possible this will be the Student Record System. Those with legitimate reason will have access to the Personal Data relevant for their job. Permissions granted for such access will be logged where possible and regularly reviewed. Other copies of personal data are discouraged, increasing the risk of a data breach or non-compliance with the appropriate Data Protection Laws. In such cases all members in possession of personal data will be required to disclose through contacting the Data Protection Officer and ensuring the registry of Data Processors is upheld.

18.4. The creation of systems and/or files which duplicate such data should be avoided; where it is inevitable every care should be taken to ensure that data maintained in subsidiary

systems is fully synchronised with definitive sources and updated frequently through secure and reliable interconnection.

18.5. All University departments should regularly review the personal files that they hold relating to individual students (whether stored electronically or in paper records) in accordance with the University's Retention and Disposal Schedule. Any failures to do so may result in the University's Disciplinary and Dismissal Policy and Procedures being invoked.

Staff Personal Data

18.6. In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by Human Resources for six years from the end of employment.

18.7. Information relating to Income Tax, Statutory Maternity Pay, etc. will be retained for the statutory time period of six years.

18.8. Staff personnel records are kept and maintained by Human Resources Department. Other departments should only keep staff information where necessary for legitimate business purposes.

18.9. To the extent that files of individual staff members are kept outside Human Resources, departments should regularly review those files in accordance with the University's Retention and Disposal Schedule.

18.10. Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for six months from the interview date and should then be destroyed as confidential waste. Human Resources may keep a record of names of individuals that have applied, been short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

19. PUBLICATION OF INFORMATION

19.1. 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.

19.2. 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 Data Protection Officer (via the Staff Portal, or email (informationcompliance@bishopg.ac.uk).

19.3. 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.

19.4. The University will normally make staff university contact details and other relevant work-related information accessible via the University's website with their consent.

19.5. Student data will be made available to relevant staff via University IT systems, Student Record System and other systems based on the information required, but access will be restricted by password and governed by the University's IT Systems Security Policy and related guidance.

Personal Data published by the University includes, but is not limited to:

19.5.1. names of all members of University Council;
19.5.2. academic staff profiles on the University website, including names, job titles and academic and/or professional qualifications and photographs;
19.5.3. Awards and Honours (including Honorary Graduands and other Honorary award recipients, Emeritus Professors and Prize-winners);
19.5.4. Staff Telephone and Email Directory;
19.5.5. Graduation programmes and videos or other multimedia versions of graduation ceremonies;
19.5.6. information in prospectuses (including photographs), annual reports, staff newsletters, etc.;
19.5.7. publicity information included in public relations stories and press releases and on social media; and
19.5.8. staff information on the University website (including photographs).

20. DIRECT MARKETING

20.1. Any proposal to carry out direct marketing (i.e. marketing by email, telephone, post or any other means that is directed at a particular individual, whether they are a student, applicant, alumnus, member of staff or otherwise) must be reviewed and approved in advance by the Director of Marketing. The Director of Marketing will seek guidance and advise from the Data Protection Officer where required.

20.2. Members of the University should not send direct marketing material to someone electronically (e.g., by email, Whatsapp, social media messenger services or targeted banner ads) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their Personal Data for direct marketing purposes.

20.3. Any department that uses Personal Data for direct marketing purposes must inform Data Subjects of this at the time of collection of the relevant Personal Data and may only make direct marketing communications where the Data Subject has opted-in to receiving such communications. Data Subjects must also be given the opportunity to opt out of receiving communications at any time and measures must be put in place to prevent such communications from being sent once the University has received confirmation that a Data Subject has opted out.

21. USING RESOURCES FOR PERSONAL USE

21.1 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.**

22. RESEARCH

22.1. 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.

22.2. 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 accordance with the recommendations of Research Councils UK, the University expects researchers to:

22.2.1. keep clear and accurate records of the research procedures followed and the results obtained, including interim results;
22.2.2. hold records securely in paper or electronic form;
22.2.3. 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;
22.2.4. manage data according to the research funder's data policy, best ethical practice and all relevant legislation;
22.2.5. wherever possible and appropriate, deposit data permanently within a national collection.

22.3. Personal Data collected only for the purposes of academic research (including work of staff and students) must be Processed in compliance with the Data Protection Laws and in compliance with the relevant research policies and its Research Ethics procedures. The University will publish additional guidance to assist researchers in complying with these requirements.

22.4. Individual students or staff conducting research should note that Personal Data may be Processed for research purposes on the legal basis that the Processing is necessary for the performance of a task conducted in the public interest or in the exercise of the official authority vested in the University. Researchers may also rely on the bases that the Processing is necessary for scientific or historical research purposes, or that it is necessary for statistical purposes.

22.5. Where the legal bases for Processing Personal Data referred to above are available to researchers, the consent of the Data Subject is **not** required. However, such Processing is subject to safeguards to ensure that data is minimised (including being pseudonymised, and if possible anonymised) and that:

22.5.1. the Personal Data are not Processed to support measures or decisions with respect to particular individuals; and
22.5.2. the Data Subjects must not be caused substantial damage or substantial distress by the Processing of the Personal Data.

22.6. If the above conditions are met, together with technical and organisational safeguards to keep data secure, Personal Data Processed for research purposes may be:

22.6.1. Processed for purposes other than that for which it was originally obtained, including statistical or historical purposes; and
22.6.2. exempt from the Data Subject's right of access and rectification, as well as their right to restrict or object to Processing.

22.7. Other than this, Data Protection Laws apply in full in respect of academic research. The obligations to collect only necessary and accurate Personal Data, to hold Personal Data securely and confidentially and not to disclose Personal Data except in accordance with the Data Protection Laws (including in relation to publication) must all still be complied with

23. PUBLICATION

23.1. Researchers should ensure that the results of research are anonymised when published and that no information is published that would allow individuals to be identified (including where anonymised data could be matched with other data to link back to an identifiable individual) where consent has not been obtained for such use from the Data Subject or, where the nature of the research makes it impracticable or otherwise undesirable to attempt to seek/obtain consent, that there is a legitimate interest in publication and publication would not unfairly damage the rights and freedoms of the Data Subject.

24. DATA PROTECTION IMPACT ASSESSMENT

24.1. The University encourages all staff to incorporate 'Privacy by Design' into their activities which involve Processing Personal Data - an approach by which data protection is built into a project from the outset, and not bolted on at the end. The Privacy Impact Assessment ("PIA") is a method by which the University can assess and address the risk of Processing and identify measures to support Data Protection.

24.2. The PIA involves setting out the envisaged Processing, its purposes, and the legal basis under which it is to be processed. It involves an assessment of the risks posed by the Processing to the rights and freedoms of the Data Subjects, and the measures to be taken to address those risks. It will include an analysis of safeguards being put in place and will demonstrate how the Processing will be compliant with the Data Protection Laws. Once the University has conducted a PIA, it will keep it under regular review to ensure that the assessment of risk addresses circumstances as they change.

24.3. To help the University meet its data protection obligations and to meet staff and students' expectations of privacy, the University carries out PIAs prior to beginning any new Processing activities where these are only required under Data Protection Laws for the large scale Processing of Sensitive Personal Data, systematic monitoring of a public area on a large scale, the systematic evaluation of individuals based on automated Processing, and other Processing activities which are likely to result in a high risk to the rights of Data Subjects. It is good practice to carry out PIAs when embarking on new projects involving the Processing of Personal Data and staff are encouraged to do so, however where this is not the case, staff are still encouraged to consider Data Protection compliance which starting any new Processing activity, to ensure it is conducted in line with this policy.

24.4. The data protection regulator in the UK also requires PIAs to be conducted where an organisation plans a number of specific Processing activities, including using new technology, processing biometric data or collecting Personal Data from a source other than the Data Subject without providing them with a privacy notice.

24.5. The PIA process is managed by the Corporate Information Team and more information can be requested via the Information Compliance Helpdesk via the Staff Portal.

25. CONCLUSION

25.1. 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.

26. LINKED POLICIES

Bishop Grosseteste University's:

- Data Breach Policy
- Privacy Policy
- Data & Information (Records) Management Policy Framework
- IT Systems Acceptable Use Policy
- Safeguarding Children and at-risk Adults Policy

The above policies are available at https://www.bgu.ac.uk/about-bgu/policies-and-procedures/policies-and-procedures-general

Relevant staff policies are available through Master Records site via SharePoint.

27. FURTHER INFORMATION

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 Corporate Information Team (informationcompliance@bishopg.ac.uk), unless they believe that the CIS team have not followed policy, in which case the Deputy Vice Chancellor (Operations) should be contacted.

If you require additional information or have questions in relation to Data Protection and best practice please contact the Data Protection Officer via email: informationcompliance@bishopg.ac.uk.