Data Protection Procedure

Policy owner:	Data Protection Officer
Implementation date:	February 2025
Review date:	Annually
Related policy:	Data Protection Policy

Index

THE UNIVERSITY OF BUCKINGHAM

Version History

Version	Author	Revisions made	Date
v.2	DPO / Legal	New Policy/Procedure Template	February 2025

1. Purpose

1.1 The purpose of this procedure is to ensure The University of Buckingham ("the University") complies with data protection laws and regulations, such as the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). These laws require companies to handle personal data responsibly and protect the privacy rights of individuals.

1.2 This procedure should be read together with:

a) Data Protection Policy;
b) Data Breach Policy and Procedure; and
c) Privacy Notice.

2. Scope

2.1 Compliance with the UK GDPR and DPA and adhering to the seven principles is the responsibility of all members of the University.

3. Procedure

3.1 Data Security

3.1.1 The University shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Data Security should be read together with the University's Policy on Use of University Computers and Data Networks.

3.1.2 The University shall ensure that the appropriate measures are taken with respect to all communications and other transfers involving personal data:

a) Personal data may be transmitted over secure networks only. Transmission over unsecured networks is not permitted in any circumstances;
b) The University will ensure that where special category personal data or other sensitive information is sent in the post that it shall be possible to demonstrate that it was delivered;
c) Where special category personal data or other sensitive information is to be sent by e-mail the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document and not in the body of the e-mail; and
d) Where personal data is to be transferred in removal storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by the University.

3.1.3 The University shall ensure that the appropriate measures are taken with respect to all communications and other transfers involving personal data:

a) All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption;
b) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

c) All personal data relating to the operations of the University, stored electronically, should be backed up on a regular basis; and
d) Where any member of staff stores personal data on a mobile device (whether that be computer, tablet, phone or any other device) then that member of staff must abide by the Use of University Computers and Data Networks of the University. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information.

3.1.4 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

3.1.5 The University shall ensure that the following measures are taken with respect to the use of personal data:

a) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the University requires access to any personal data that they do not already have access to, such access should be formally requested from;
b) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the University or not, without the initial authorisation of the DPO;
c) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
d) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
e) Where personal data held by the University is used for marketing purposes, it shall be the responsibility of the relevant department to ensure that the appropriate consent is obtained and that no data subjects have opted out.

3.1.6 The University shall ensure that the following measures are taken with respect to the use of personal data:

a) The University requires that any passwords used to access personal data shall have a minimum of 10 characters, composed of a mixture of upper and lower case characters, numbers and symbols. Passwords are not expected to be changed upon a regular basis but users will be expected to change their password if instructed by the University;

b) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the University, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

c) All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The University ’s IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;

d) No software may be installed on any Company-owned computer or device without the prior approval of IT Services; and

e) Where members of staff or other user use online applications that require the use of personal data, the use of that application must be signed off by IT Services.

3.2 **Data Retention**

3.2.1 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected.

3.2.2 Once information is no longer needed it should be disposed of securely. Paper records should be shredded or disposed of in confidential waste and electronic records should be permanently deleted.

3.2.3 If data is fully anonymised then there are no time limits on storage.

3.3 **Lawful Basis for Processing**

3.3.1 The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

a) The data subject has given consent to the processing of their personal data for one or more specific purposes. Anyone who has provided consent has the right to revoke their consent at any time and must be informed of that right;

b) The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

c) The processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) The processing is necessary to protect the vital interests of the data subject or of another natural person;

e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.3.2 All processing of personal data carried out by the University must meet one or more of the conditions above. In addition the processing of 'special categories' of personal data requires extra, more stringent, conditions to be met in accordance with Article 9 of the DPA AND UK GDPR. To process personal data about criminal convictions or offences, conditions must be met under Article 10 DPA and UK GDPR.

3.3.3 The University is a privately funded charitable institution and, as such does not fall within the definition of Public Authority for the purposes of the DPA and UK GDPR.

3.4 Accuracy of data and Keeping Data Up to Date

3.4.1 The University shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

3.4.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

3.5 Privacy Notices

3.5.1 Under the 'fair and transparent' requirements of the first data protection principle, the University is required to provide data subjects with 'privacy notices' to inform them what the University does with their personal data.

3.5.2 The University Privacy Notice is published on the University website and available to individuals from their first point of contact with the University. Any processing of personal data beyond the scope of the University's Privacy Notice will require a separate privacy notice and the Data Protection Officer should be notified of the proposed activity beforehand to ensure such processing is in accordance with this policy and the UK GDPR AND DPA.

3.6 Records of Processing Activities

3.6.1 As a data controller, the University is required to maintain a record of processing activities ("ROPA") which covers all the processing of personal data carried out by the University. Amongst other things this record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU.

3.6.2 Staff undertaking a new activity involving the use of personal data that is not covered by one of the existing records of processing activities should inform the Data Protection Officer (data-protection@buckingham.ac.uk) before starting the new activity.

3.7 Children

3.7.1 Under UK GDPR AND DPA there are restrictions that apply to the processing of personal information relating to children. Although the University does not generally process the data of children, there may be circumstances when it is necessary to do so. If it is deemed necessary within any school or department of the University to process the personal data of children, the Data Protection Officer should be consulted prior to the processing activities to ensure that necessary steps are taken to ensure that such processing is in accordance with the UK GDPR AND DPA.

3.8 Research

3.8.1 Data collected for the purposes of research is covered by the UK GDPR AND DPA. It is important that staff collecting data for the purpose of research or consultancy incorporate an appropriate form of consent on any data collection form.

3.9 Data Sharing

3.9.1 Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of the University.

3.9.2 As a general rule personal data should not be passed on to third parties, particularly if it involves special categories of personal data. It is however permissible or necessary in certain circumstances. Any transfers of personal data must meet the data processing principles, in particular it must be lawful and fair to the data subjects concerned. More particularly:

- It must meet one of the conditions of processing (see section 3.3);
- Legitimate reasons for transferring data (e.g. legal requirement);
- The University must be satisfied that the third party will meet all the requirements of UK GDPR AND DPA particularly in terms of holding the information securely; and
- where a third party is to process personal data on behalf of the University, a written contract must be in place containing appropriate Data Protection safeguards.

3.9.3 Staff should consult with the Data Protection Officer and Legal Services if they are entering into a new contract that involves the sharing or processing of personal data or if they have any concerns about the Data Protection safeguards in existing contracts.

3.9.4 Staff should consult the Data Protection Officer if they receive requests for personal information from third parties (e.g., police, local councils etc).

3.10 Transferring Personal Data to a Country without an Adequacy Decision

3.10.1 The University may transfer ('transfer' includes making available remotely) personal data to countries without a suitable adequacy decision from the UK Government.

3.10.2 The transfer of personal data to a country without an adequacy decision shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK Government has determined ensures an adequate level of protection for personal data;
b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK Government compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted

into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) The transfer is made with the informed consent of the relevant data subject(s);
d) The transfer is necessary for the performance of a contract between the data subject and the University (or for pre-contractual steps taken at the request of the data subject);
e) The transfer is necessary for important public interest reasons;
f) The transfer is necessary for the conduct of legal claims;
g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

3.10.3 Information published on the internet must be considered to be an export of data outside the EU. This covers data stored in the cloud unless the service provider explicitly guarantees data storage only takes place within the EU. Presently the University does not utilise any cloud storage outside of the EU.

3.10.4 The Information Commissioner's Office Guidance on the use of Cloud Computing should be consulted before any use of external computing resources or services via a network which may involve personal data takes place.

3.11 **Data Protection Impact Assessments**

3.11.1 A Data Protection Impact Assessment (DPIA) must be completed before a project begins or, at the very latest, during the planning phase. The key idea is to assess and mitigate any data protection risks prior to processing personal data, not after.

3.11.2 Before Starting the Project: If you're planning a project that involves processing personal data and the processing is likely to result in a high risk to the rights and freedoms of individuals (e.g., using new technology, large-scale data processing, profiling, etc.), a DPIA should be done before the processing begins. This allows you to identify and address potential risks to data subjects' privacy and data protection rights at the outset.

During the Planning Phase: The DPIA should ideally be integrated into the early stages of the project, during the planning or design phase. This enables you to consider privacy and data protection in the design (the concept of "Privacy by Design and by Default").

The UK GDPR requires that the DPIA be conducted whenever there are high risks involved in the processing activities, such as when new technologies are being introduced or when data processing is likely to impact individuals' privacy significantly.

If a DPIA identifies high risks that cannot be mitigated, you must consult the Registrar & Chief Administrative Officer with committee oversight from the Executive Group and Audit & Risk Committee before starting the processing.

3.12 **Data Protection by Design**

3.12.1 It is particularly important to consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data. UK GDPR AND DPA imposes a specific 'Privacy by Design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.

3.13 **Data Breach Notification**

3.13.1 The University is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The University must make every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions.

3.13.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

3.13.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

3.13.4 If a data protection breach occurs you must contact the Data Protection Officer immediately and follow the Data Breach Procedure.

3.13.5 Examples of common personal data breaches include:

- Loss or theft of data or equipment on which data is stored or accessible;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to the incorrect recipient);
- Human error; and
- Failure to maintain effective firewalls resulting in successful hacking attacks.

3.14 **Direct Marketing**

3.14.1 Direct marketing is defined as the communication of advertising or marketing material directed to particular individuals.

3.14.2 The University may contact prospective, current and former students for the purpose of direct marketing and fundraising. The University may also contact individuals who have expressed an interest or who have been identified by information which is publicly available as a potential donor or customer.

3.14.3 This means that the University may use personal data that it has collected in accordance with this Policy to contact individuals about events that they have registered for, products that they have purchased (or that have been purchased for them), reminders regarding courses, to tell them about the University's products available from time to time and to raise funds for approved projects.

3.14.4 The direct marketing communications may be provided through Social Media Channels, email, post, SMS or such other means as the University chooses.

3.14.5 When collecting data that will be used for marketing purposes directly from individuals, the University will state whether it will use the data for direct marketing purposes.

3.14.6 Individuals will be provided with the opportunity to opt out receiving these direct marketing communications at any time.

3.14.7 The University will not necessarily remove personal data from its database(s) if it considers it is necessary to retain the personal data for another legitimate purpose (e.g. because it is necessary to administer a contract or because it is a legal requirement).

3.14.8 Direct marketing must also comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) which covers marketing via telephone, text and email.

3.15 **Data Subject Rights**

3.15.1 **Keeping Data Subjects Informed:** The University shall provide to every data subject:

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

    a. if the personal data is used to communicate with the data subject, when the first communication is made; or
    b. if the personal data is to be transferred to another party, before that transfer is made; or
    c. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided:

a) Details of the University including, but not limited to, the identity of its Data Protection Officer;

b) The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which the University is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located in a territory without an adequacy agreement as approved by the UK Government, details of that transfer, including but not limited to the safeguards in place;

g) Details of data retention;

h) Details of the data subject's rights under the UK GDPR;

i) Details of the data subject's right to withdraw their consent to the University's processing of their personal data at any time;

j) Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK GDPR);

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

l) Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

3.15.2 **Data Subject Access Request:** Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the University holds about them, what it is doing with that personal data, and why.

Individual's wishing to make a SAR should contact the Data Protection Officer (data-protection@buckingham.ac.uk).

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

The University does not charge a fee for the handling of normal SARs. The University reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

To ensure compliance with our legal obligations to protect third party personal data. The University can apply the third-party exemption under the Data Protection Act 2018, Schedule 2, Part 3, Paragraph 16 to redact information that is confidential to the University.

3.15.3 **Rectification of Personal Data:** Data subjects may have the right to require the University to rectify any of their personal data that is inaccurate or incomplete.

Where such rectification is possible, The University shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the University of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

3.15.4 **Erasure of Personal Data:** Data subjects have the right to request that the University erases the personal data it holds about them in the following circumstances:

a. It is no longer necessary for the University to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
b. The data subject wishes to withdraw their consent to the University holding and processing their personal data;
c. The data subject objects to the University holding and processing their personal data (and there is no overriding legitimate interest to allow the University to continue doing so) (see 3.15.7 for further details concerning the right to object);
d. The personal data has been processed unlawfully;
e. The personal data needs to be erased in order for the University to comply with a particular legal obligation.
f. Unless the University has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
g. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

3.15.5 **Restriction of Personal Data Processing:** Data subjects may request that the University restricts processing the personal data it holds about them. If a data subject makes such a request, the University shall in so far as is possible ensure that the personal data is only stored and not processed in any other means.

If the University is required to process the data for statutory purposes or for reasons of legal compliance, then the University shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

3.15.6 **Data Portability:** The University processes personal data using automated means.

Where data subjects have given their consent to the University to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the University and the data subject, data subjects have the right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

3.15.7 **Objections to Personal Data Processing:** Data subjects have the right to object to the University processing their personal data based on performing a task in the public interest. Its' legitimate interests, or direct marketing (including profiling)

Where a data subject objects to the University processing their personal data, the University shall cease such processing immediately, unless it can be demonstrated that the University's grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the University processing their personal data for direct marketing purposes, the University shall cease such processing immediately.

Where a data subject objects to the University processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, "demonstrate grounds relating to his or her particular situation". The University is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

3.15.8 **Automated Decision-Making:** The University may use personal data in automated decision-making processes. In the event that that this situation occurs, the University shall notify data subjects of its' intentions to commence such processing.

Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the UK GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the University.

The right described above does not apply in the following circumstances:

a. The decision is necessary for the entry into, or performance of, a contract between the University and the data subject;
b. The decision is authorised by law; or
c. The data subject has given their explicit consent.

3.15.9 **Profiling:** The University uses personal data for profiling purposes. These purposes relate to helping student maximise achievement and monitor staff performance.

When personal data is used for profiling purposes, the following shall apply:

a. Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
b. Appropriate mathematical or statistical procedures shall be used;
c. Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
d. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling

The availability of rights largely depends on the legal justification for processing. The table below summarises when rights are available.

	Right to:				
Legal Justification	**Object**	**Erasure**	**Automated Decision Making**	**Rectification**	**Portability**
Consent	No (but can withdraw consent)	Yes	No (but can withdraw consent)	Yes	Yes
Contract	No	Yes	No	Yes	Yes
Legal Obligation	No	No	No	Yes	No
Vital Interest	No	Yes	No	Yes	No
Public Task	Yes	No	Yes	Yes	No
Legitimate Interests	Yes	Yes	Yes	Yes	No

Any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month of receiving the request. Members of staff should consult the Data Protection Officer for advice if they encounter any difficulty in complying with a request. It is possible to extend the time for compliance by a further two months where requests are complex or numerous in which event it is necessary to inform the individual within one month of the receipt of the request and explain why the extension is necessary.

3.16 **Organisational Measures**

3.16.1 The University shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the University shall be made fully aware of both their individual responsibilities and our responsibilities under the UK GDPR and under this Policy, and shall have free access to a copy of this Policy;

b) Only employees, agents, sub-contractors, or other parties working on behalf of the University that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the University;

c) All employees, agents, contractors, or other parties working on behalf of the University handling personal data will be appropriately trained to do so;

d) All employees, agents, contractors, or other parties working on behalf of the University handling personal data will be appropriately supervised;

e) All employees, agents, contractors, or other parties working on behalf of the University handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) All personal data held by the University shall be reviewed periodically, as set out in the University's Data Retention Policy;

h) The performance of those employees, agents, contractors, or other parties working on behalf of the University handling personal data shall be regularly evaluated and reviewed;

i) The contravention of these rules will be treated as a disciplinary matter;

j) All employees, agents, contractors, or other parties working on behalf of the University handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy by contract;

k) All agents, contractors, or other parties working on behalf of the University handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the University arising out of this Policy and the UK GDPR; and

l) Where any agent, contractor or other party working on behalf of the University handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the University against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

3.17 **Impact of Non-Compliance**

3.17.1 All staff and students of the University are required to comply with this Data Protection Policy and Procedure, its supporting guidance and the requirements specified in the UK GDPR AND DPA.

3.17.2 Any member of staff or student who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy and Procedure may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of the University for their own purposes, which are outside the legitimate purposes of the University.

3.17.3 The University could be fined for non-compliance of the UK GDPR AND DPA.

3.18 **University Contacts**

3.18.1 The University's named Data Protection Officer is Hahna Akhtar whose contact details are as follows:

Email: data-protection@buckingham.ac.uk
Address: Data Protection Officer, University of Buckingham, Buckingham MK18 1EG

3.18.2 In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to the Data Protection Officer. The decision to seek specialist external legal advice on the matter will be at the discretion of the Data Protection Officer.

Annex A: Data Subject Rights

1. **Right to be informed**
2. **Right of access (data subject access request)**
3. **Right to rectification**
4. **Right to erasure (right to be forgotten)**
5. **Right to restrict processing**
6. **Right to data portability**
7. **Right to object**
8. **Rights in relation to automated decision making and profiling**