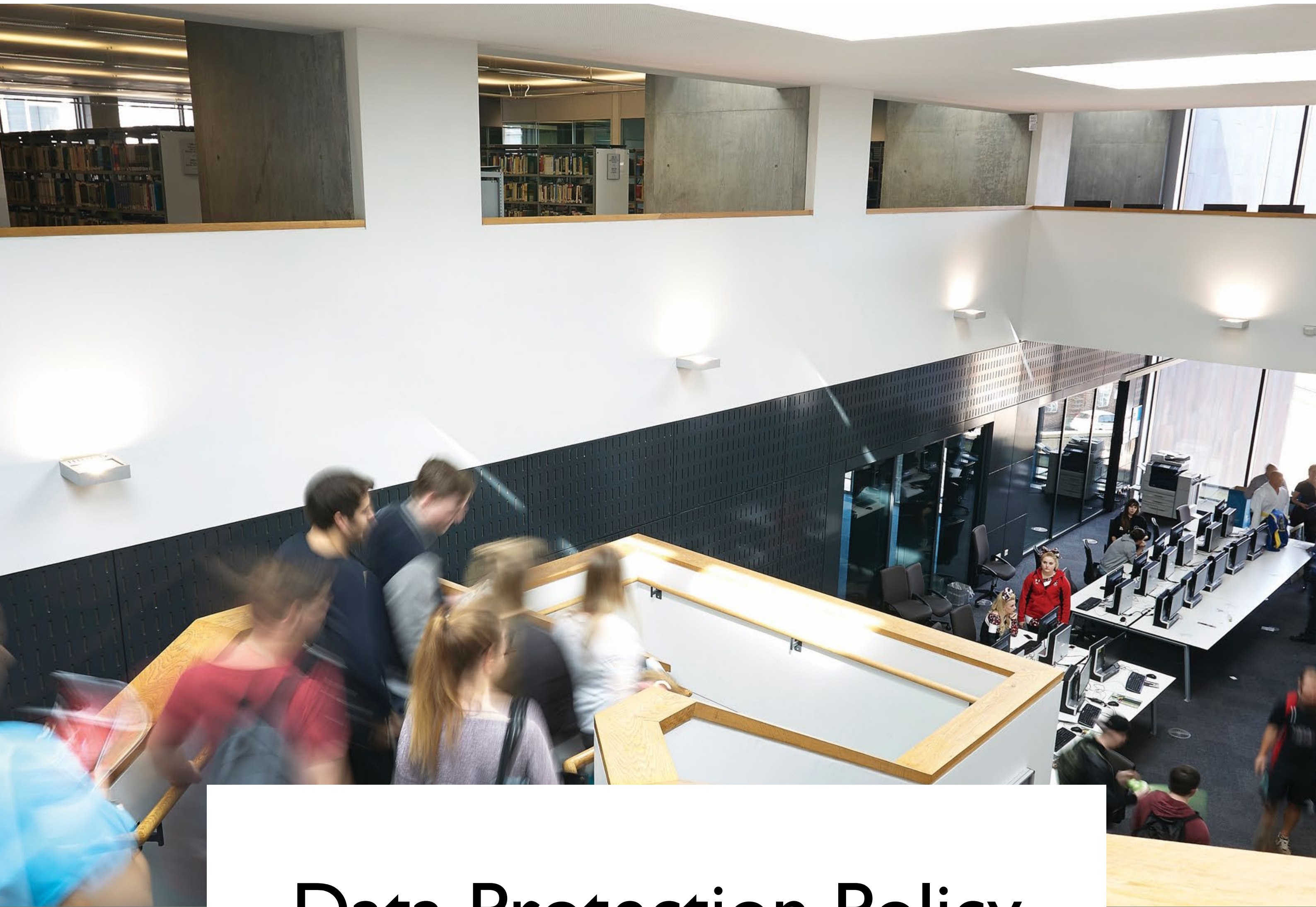
BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891



Data Protection Policy

Contents

Approved by:	Digital Experience Steering Group	**Date first published:**	Jun-2017
Version:	0.7	**Date updated:**	Jun-2022
Owner:	Data Protection Officer	**Review Date:**	Jun-2024

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the University Secretariat.

Purpose

1 Buckinghamshire New University holds and processes personal data about its staff, students and other data subjects for academic, administrative and commercial purposes and also to fulfil statutory obligations to the government and other statutory bodies.

2 The University processes personal information to enable it to provide education and support services to students and staff; advertising and promoting the university and the services we offer; publication of the university magazine and alumni relations, undertaking research and fundraising; managing our accounts and records and providing commercial activities to our clients. We also process personal information for the use of CCTV systems to monitor and collect visual images for the purposes of security and the prevention and detection of crime.

3 Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. The University is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose the University to complaints, regulatory action, fines and/or reputational damage.

4 This policy should be read in conjunction with the Data Quality Policy as all staff must make every effort to ensure that any data collected or entered into our systems is accurate, valid, reliable, timely and relevant.

Applicability and Scope

5 This policy applies to all University employees. All University staff are expected to be familiar with this policy and comply with its terms.

6 This policy applies to all processing of personal data in electronic form (including databases, electronic mail and unstructured electronic documents) or where it is held in paper based manual files that are structured in a way that allows ready access to information about individuals.

7 It also applies regardless of where data is held if the data is being processed for University purposes, (for example, it covers data held on off and on premise and on mobile devices such as on electronic tablets, laptops or mobile phones) and regardless of who owns the device on which it is stored.

8 The University is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct. This policy sets forth the expected behaviours of staff and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data.

Definitions

9 **Personal Data** is any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, cardholder data, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

10 **Sensitive Personal Data** includes information relating to racial or ethnic origin, disability, political opinions, religious beliefs, trade union membership, health, sex life, and criminal

convictions. The processing of sensitive personal data is subject to much stricter conditions. It is expected that we would need to gain explicit consent for this type of data and keep robust records of this consent.

11 **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

12 **Data Controller** is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

13 **Data Processor** is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

14 **Consent of the Data Subject** means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Protection Principles

15 The following principles underpin the provisions in this policy and have been adopted by the University to govern the way it processes Personal Data:

a) **Principle 1: Lawfulness, Fairness and Transparency -** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, the University must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

b) **Principle 2: Purpose Limitation -** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the University must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

c) **Principle 3: Data Minimisation -** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the University must not store any personal data beyond what is strictly required.

d) **Principle 4: Accuracy -** Personal data shall be accurate and kept up to date. This means the University must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

e) **Principle 5: Storage Limitation -** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means the University must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

f) **Principle 6: Integrity and Confidentiality -** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The

University must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

g) **Principle 7: Accountability -** The data controller shall be responsible for, and be able to demonstrate compliance. This means the University must demonstrate that the six Data Protection Principles above are met for all personal data for which it is responsible.

Processing of Personal Data

16 The University will hold the minimum personal data necessary for it to perform its functions, and the data will be erased once the need to hold it has passed in accordance with the recommended retention periods.

17 Wherever possible, manual or computerised personal data will be held in one location only, with a named responsible person, to assist compliance with the data protection legislation. This will provide for improved security of data, consistency of data sets, ease of access for data subjects and confirmation of explicit (written) consent for sensitive data or that transmitted outside the EEA.

18 Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected without undue delay.

19 Personal data will be treated as confidential and will be processed in accordance with the provisions of the Data Protection Act and the University's notification under it.

20 Other than for the purposes of normal University business or as a result of a statutory or legal obligation, personal data must not be disclosed to an unauthorised third party.

21 Individuals as well as University can be prosecuted for breaches of the Act. The University will take all reasonable steps to provide training and guidance in the use of personal data and will review its systems and procedures accordingly.

Responsibilities

22 The University as a corporate body is the data controller. The senior officer responsible for the ensuring that the University is compliant with Data Protection Act is the Data Protection Officer.

23 The University's Data Protection Officer oversees the implementation of the Data Protection Policy in accordance with the provisions of the Data Protection Act. The Data Protection Officer for the University is the Director of Digital and Technical Services (DTS).

24 All staff and students are responsible for ensuring that:

a) Personal data is processed in compliance with the University's Data Protection Policy and supporting guidance.

b) Personal data is processed in accordance with requirements of the Data Protection Act and the Data Protection Principles.

c) The data subject consents to their data being used and knows what it will be used for.

d) Personal data is not collected for one purpose and subsequently used for another (for example, using contact details provided for HR related purposes for marketing).

e) Personal data is not disclosed to a third party outside of the University without the consent of the data subject.

f) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party.

g) Personal data relating to data subjects is only ever processed for approved work, research or study related purposes.

h) Comments or other data about individuals, which they would not be comfortable about the individual seeing, are not recorded, either in emails or elsewhere because data subjects have the right to see their personal data.

i) Personal data which comes into their possession is always kept and disposed of securely.

j) Information is disposed of correctly making sure that it is permanently removed from servers and that hard copies of information are confidentially shredded and not disposed of in a wastepaper basket/recycle bin.

k) Any information provided to the University in connection with their enrolment or employment is accurate and up-to-date and that the University notified promptly of any changes to their personal data (for example, change of address or emergency contact details).

l) The use of the information is necessary for a relevant purpose, is not retained longer than necessary and is kept in accordance with the University's retention schedule.

m) Advice is sought from their line manager, senior management or the Data Protection Officer if there is any doubt about what do with personal data.

n) They are familiar with and comply with the University's Information Security, Acceptable User Policy and Mobile Data Device Use policies if they are working remotely or using a mobile device to store data (for example, a laptop, tablet or mobile phone), it is vital that.

o) A Data Protection Impact Assessment is carried for any new initiative where the processing of personal data is being considered and advice is sought if any data protection related concerns are raised.

p) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to Data Protection Officer.

q) Any personal information received in error by whatever means, is reported to the Data Protection Officer immediately and that it is handled by the appropriate individual within the University.

Data Protection Breaches

25 Staff and students must ensure that any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support the Data Protection Officer in resolving breaches.

26 If an individual finds any lost or discarded data which they believe contains personal data, (for example, a memory stick) they must report the matter to their line manager and report it to the Data Protection Officer immediately.

27 If an individual becomes aware that personal data has been accidentally lost, stolen or inadvertently disclosed (for example, if their laptop or phone containing personal data is lost),

they must report the matter immediately to their line manager and to the Data Protection Officer.

28 Any member of staff or student who considers that the Data Protection Policy has not been followed in respect of personal data about them, should raise the matter with the Data Protection Officer or HR Services Director initially. If the matter cannot be resolved informally then staff and students have recourse to the Staff Grievance Procedure or the Student Complaints Procedure respectively.

Personal Data in the Public Domain

29 The University holds certain information about staff and students in the public domain like for example on the University web site or in publications. Personal data classified as being in the 'public domain' refers to information that is already publically available and may be disclosed to third parties without having to seek consent from the data subject.

30 The University will make some personal data publically available unless individuals have objected, like for example: names, work place email addresses, telephone numbers, academic qualifications, biographies and curricula vitae of academic staff, support staff, Council members and Senate members where supplied and where appropriate.

31 The University may process personal information about third parties which is already in the public domain where such processing is carried out in accordance with the Data Protection Act principles and is unlikely to cause any damage or distress to the data subject.

Data security

32 Keeping personal data secure is a requirement of the Data Protection Act and all staff are therefore responsible for familiarising themselves with the University's Information Security Policy and ensuring that:

a) Any personal data they hold is kept securely and is not disclosed (either orally or in writing) to any unauthorised third party.

b) Any personal data recorded in paper form or hard copy documents are kept in locked filing cabinets, drawers and offices.

c) Any portable devices (e.g. memory sticks) on which personal data is stored are encrypted, kept in a secure location and transferred from one place to another with care to avoid accidental loss.

d) Mobile devices used to access or store personal data are properly password protected and where appropriate encrypted.

Rights to Access Information

33 Individuals have the right to access any personal data that relates to them which the University holds. They also have the right to object to processing, automated decision-making and profiling. They can restrict processing and have the right to data portability, rectification and erasure. Any person who wishes to exercise these right should see the Detailed Guidance section.

34 The University will consider requests relating to any of the rights listed above in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and complying with such a request unless the request is deemed to be excessive in nature.

35 All requests received for access to or rectification of personal data must be made in writing and directed to the Data Protection Officer, who will log each request as it is received and ensure the appropriate areas respond to requests.

36 Appropriate verification must confirm that the requestor is the data subject or their authorised legal representative. A response to each request will be provided within 30 days of the receipt of the written request from the data subject.

Research

37 Before commencing any research which will involve obtaining or using personal data, the researcher and their supervisor must give due consideration to this policy and supporting guidance. For more information refer to the Research Data Policy.

38 Researchers and supervisors must consider the type of personal data which may be collated, how consent is to be recorded, the extent to which such data may legitimately be required for the academic objective, how the data will be securely stored, (particularly if the data is what might be considered to be sensitive) and the duration for which it will be retained.

39 Personal data processed for research should be limited to the minimum amount of data which is reasonably required to achieve the desired academic objectives and wherever possible any such personal data should be made anonymous so that the data subjects cannot be identified.

Enforcement

40 Any actual or suspected breach of this policy must be reported to the Director of DTS via the most suitable channel. The Director of DTS will take appropriate action and inform the relevant internal and external authorities.

41 Failure to comply with this policy may result in disciplinary action in accordance with the relevant process.

Detailed Guidance: Data Collection

42 Personal data should be collected only from the data subject unless one of the following apply:

a) The nature of the business purpose necessitates collection of the personal data from other persons or bodies.

b) The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

43 If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

a) The data subject has received the required information by other means.

b) The information must remain confidential due to a professional secrecy obligation

c) A national law expressly provides for the collection, processing or transfer of the personal data.

44 Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than one calendar month from the first collection or at the time of first communication or at the time of disclosure.

Detailed Guidance: Data Subject Consent

45 The University will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned.

46 The University shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data. The system must include provisions for:

a) Determining what disclosures should be made in order to obtain valid consent.

b) Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.

c) Ensuring the consent is freely given (i.e. is not based on a contract that is conditional to the Processing of personal data that is unnecessary for the performance of that contract).

d) Documenting the date, method and content of the disclosures made, as well as the validity, scope, and preference of the consents given.

e) Providing a simple method for a data subject to withdraw their consent at any time.

Detailed Guidance: Data Subject Notification

47 The University will provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be given orally, electronically or in writing. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

48 Each external website provided by a University will include an online ‘Privacy Notice’ and an online ‘Cookie Notice’ fulfilling the requirements of applicable law. All Privacy and Cookie Notices must be approved by the Data Protection Officer prior to publication on the external website.

Detailed Guidance: Data Processing

49 The University uses personal data for the general running of the organisation and business administration as detailed in the notification with the Information Commissioner’s Office.

50 The use of a contact’s information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

51 The University will process personal data in accordance with all applicable laws and applicable contractual obligations and will not process personal data unless at least one of the following requirements are met:

a) The data subject has given consent to the processing of their personal data for one or more specific purposes.

b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

c) Processing is necessary for compliance with a legal obligation to which the data controller is subject.

d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

e) 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.

f) 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 interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

52 There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

53 In any circumstance where consent has not been gained for the specific processing in question, the University will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected:

a) Any link between the purpose for which the personal data was collected and the reasons for intended further processing.

b) The context in which the personal data has been collected, in particular regarding the relationship between data subject and the data controller.

c) The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.

d) The possible consequences of the intended further processing for the data subject.

e) The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

Detailed Guidance: Processing of Special Categories of Data

54 The University will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:

a) The processing relates to personal data which has already been made public by the data subject.

b) The processing is necessary for the establishment, exercise or defence of legal claims.

c) The processing is specifically authorised or required by law.

d) The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

e) Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

55 Where special categories of data are being processed, the University will adopt additional protection measures. For example, prior approval must be obtained and the basis for the Processing clearly recorded with the personal data in question.

56 Children are unable to consent to the processing of personal data for information society services. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Detailed Guidance: Data Quality

57 The University will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject as set out in the Data Quality Policy.

Detailed Guidance: Profiling and Automated Decision-Making

58 The University will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where the University uses profiling and automated decision-making, this will be disclosed to the relevant data subjects.

Detailed Guidance: Digital Marketing

59 The University will not send promotional or direct marketing material to a data subject through digital channels such as mobile phones, email and the Internet, without first obtaining their consent.

60 Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes.

61 If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately and their details should be kept on a suppression list with a record of their opt- out decision, rather than being completely deleted.

Detailed Guidance: Data Retention

62 To ensure fair processing, personal data will not be retained by the University for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

63 The length of time for which the University needs to retain personal data is set out in the University's Record Management Policy and Records Lifecycle Management Scheme. This takes into account the legal and contractual requirements that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Detailed Guidance: Information Security and Data Protection

64 The University will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment as set out in the University's Information Security Policy.

Detailed Guidance: Data Subject Requests

65 The University will establish a set of procedures to enable and facilitate the exercise of data subject rights related to:

a) Information access.

b) Objection to Processing.

c) Objection to automated decision-making and profiling.

d) Restriction of Processing.

e) Data portability.

f) Data rectification.

g) Data erasure.

66 The University will consider requests relating to any of the rights listed above by an individual in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

67 Data subjects shall have the right to require the University to correct or supplement erroneous, misleading, outdated, or incomplete personal data and are entitled to obtain the following information about their own personal data:

a) The purposes of the collection, processing, use and storage of their personal data.

b) The source(s) of the personal data, if it was not obtained from the data subject;

c) The categories of personal data stored for the data subject.

d) The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients.

e) The envisaged period of storage for the personal data or the rationale for determining the storage period.

f) The use of any automated decision-making, including profiling.

g) The right of the data subject to:

    i. Object to processing of their personal data.

    ii. Lodge a complaint with the Data Protection Authority (i.e. Information Commissioner's Office).

    iii. Request rectification or erasure of their personal data.

    iv. Request restriction of processing of their personal data.

68 All requests received for access to or rectification of personal data must be made in writing and directed to the Data Protection Officer, who will log each request as it is received. Appropriate verification must confirm that the requestor is the data subject or their authorised legal representative. A response to each request will be provided within 30 days of the receipt of the written request from the data subject.

69 If the University cannot respond fully to the request within 30 days, the Data Protection Officer shall nevertheless provide the following information to the data subject, or their authorised legal representative within the specified time:

a) An acknowledgement of receipt of the request.

b) Any information located to date.

c) Details of any requested information or modifications which will not be provided to the data subject, the reason(s) for the refusal, and any procedures available for appealing the decision.

d) An estimated date by which any remaining responses will be provided.

e) An estimate of any costs to be paid by the data subject (e.g. where the request is excessive in nature).

f) The name and contact information of the individual in the University who the data subject should contact for follow up.

70 It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Detailed Guidance: Law Enforcement Requests and Disclosures

71 71 In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

a) The prevention or detection of crime.

b) The apprehension or prosecution of offenders.

c) The assessment or collection of a tax or duty.

d) By the order of a court or by any rule of law.

72 If the University processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

73 If any employee of the University receives a request from a court or any regulatory or law enforcement authority for information relating to a Data Subject, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

Detailed Guidance: Transfers to Third Parties

74 The University will only transfer personal data to, or allow access by, third parties (including Cloud Computing services), when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, the University will first identify if, under applicable law, the third party is considered a data controller or a data processor of the personal data being transferred.

75 Where the Third Party is deemed to be a data controller, the University will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the personal data transferred, using an Information Sharing Agreement.

76 Where the Third Party is deemed to be a data processor, the University will enter into an adequate processing agreement with the data processor in the form of the Buckinghamshire New University Data Processing and Information Security Agreement to ensure that the data processor implements the appropriate technical and organisational measures to protect the personal data.

77 The University shall conduct regular audits of processing of personal data performed by third parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by the Digital Experience Steering Group (DESG).

Detailed Guidance: Data Transfers to another Country

78 The University may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Transfers made to countries lacking an adequate level of legal protection need to be completed in compliance with the applicable law.

Detailed Guidance: Complaints Handling

79 Data subjects with a complaint about the processing of their personal data, should put the matter forward in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

80 If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their discretion, seek redress through mediation, binding arbitration, litigation, or via complaint to the Information Commissioner's Office.

Detailed Guidance: Breach Reporting

81 Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can me made via e-mail IT@bucks.ac.uk or by calling 01494 605000.

82 The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the Information Security Incident Procedure.

Detailed Guidance: Responsibilities

83 The Data Protection Officer is the Director of DTS and is accountable for the implementation of this policy in the University and will be responsible for:

a) Keeping DESG updated about data protection responsibilities, risks and issues.

b) Reviewing all data protection procedures and policies on a regular basis.

c) Arranging data protection training and advice for all staff members and those included in this policy.

d) Answering questions on data protection from staff, board members and other stakeholders.

e) Responding to individuals such as clients and employees who wish to know which data is being held on them by the University.

f) Checking and approving third parties that handle the company's data any contracts or agreement regarding data processing.

g) Ensure all systems, services, software and equipment meet acceptable security standards.

h) Checking and scanning security hardware and software regularly to ensure it is functioning properly.

i) Researching third-party services, such as cloud services the company is considering using to store or process data.

Detailed Guidance: Data Protection Training

84 All University employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. The University will provide regular data protection training and procedural guidance for staff.

Detailed Guidance: Data Protection by Design

85 To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

86 Each department must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer for all new and/or revised systems or processes for which it has responsibility.

87 The subsequent findings of the DPIA must then be submitted to Data Protection Officer for review and approval. Where applicable, the DTS Directorate will assess the impact of any new technology uses on the security of personal data.

High Wycombe Campus
Queen Alexandra Road
High Wycombe
Buckinghamshire
HP11 2JZ

Aylesbury Campus
59 Walton Street
Aylesbury
Buckinghamshire
HP21 7QG

Uxbridge Campus
106 Oxford Road
Uxbridge
Middlesex
UB8 1NA

BNU based at
Pinewood Studios

Pinewood Studios
Pinewood Road
Iver Heath
Buckinghamshire
SL0 0NH

Missenden Abbey
London Road
Great Missenden
Buckinghamshire
HP16 0BD

Telephone: 01494 522 141

BucksNewUni

BucksNewUni

BucksNewUni

BucksNewUniversity

If you have any queries about this policy, please contact the School or Directorate responsible for the policy