Introduction

Index

Introduction ................................................................................................................................... 2
Policy Statement .......................................................................................................................... 3
Breaches of Policy ........................................................................................................................ 3
The Data Controller* ..................................................................................................................... 4
Data Protection Officer (DPO)* ..................................................................................................... 4
Notification of data* held and processed* ..................................................................................... 4
Responsibilities ............................................................................................................................ 4
Student Responsibilities ............................................................................................................... 6
Brighton and Sussex Medical School (BSMS) .............................................................................. 7
Data Subject Rights - Staff and student data ................................................................................ 7
  Subject Access request ............................................................................................................. 7
  Examination Scripts ................................................................................................................. 7
The right to complain to the ICO ................................................................................................... 8
Data Breach .................................................................................................................................. 8
  Data breach reporting ............................................................................................................... 9
International Data Transfers ......................................................................................................... 9
Sharing of Personal Data ............................................................................................................. 9
  Working with third parties who process data on our behalf ...................................................... 10
Research and consultancy ......................................................................................................... 11
Social Media ................................................................................................................................ 11
CCTV ......................................................................................................................................... 12
Retention of data ........................................................................................................................ 12
  Student records ...................................................................................................................... 12
  Staff records .......................................................................................................................... 13
Conclusion ................................................................................................................................. 13
Policy Review and Maintenance ................................................................................................. 13
Related Policies .......................................................................................................................... 13
Related Guidance ....................................................................................................................... 13
Appendix 1 Glossary of Data Protection Terms .......................................................................... 14
Appendix 2 Data Protection Principles ........................................................................................ 15
Appendix 3 Use of Staff Images ................................................................................................. 16
Appendix 4 Unicard .................................................................................................................... 18
  Konica Minolta MFDs .............................................................................................................. 19
  Access Control Records .......................................................................................................... 19

Introduction
The University of Brighton needs to process certain personal information in order to deliver its core teaching and learning functions, operate effectively as an organisation and meet legislative, contractual and statutory obligations. The information its processes includes personal data relating to applicants, students, employees, alumni, friends, supporters, partners, suppliers, research participants and many others.

The University of Brighton is committed to openness and accessibility in the provision of information for all aspects of its work, having due regard to issues of efficiency, legality, security and confidentiality. This policy has been written to provide demonstrable commitment to the legal requirements in the handling of personal information under the Data Protection Act 2018 (the “DPA”). Compliance with this legislation also enables efficient working practices, and significantly reduces the likelihood of an information or security breach and its wider effects that could include harm/distress to data subjects, reputational damage, financial penalties or compensation, and investigations by the Information Commissioner.

Items marked * are defined in the glossary of terms at Appendix 1.

**Policy Statement**

The University of Brighton and all staff who process or use any personal information will ensure that personal data is processed in accordance with the following data protection principles (Appendix 2):

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

**Breaches of Policy**

All breaches of this policy and data protection legislation shall be reported immediately to the Data Protection Officer.

Third parties shall report via their University point of contact.
A deliberate or negligent breach of this policy by an employee or student may result in disciplinary action being taken following an appropriate investigation. Where a supplier fails to comply with the policy or any associated data protection condition it may result in termination for breach of contract and/or result in a claim for compensation.

**The Data Controller***

The University of Brighton is the data controller under the DPA and is responsible for ensuring compliance with the principles of data protection legislation.

In matters of collaboration and partnership with other bodies, it is possible for either or both organisations to be the data controller, depending upon the nature of the agreement or contract. Please refer any queries to the Head of Data Compliance and Records Management.

**Data Protection Officer (DPO)***

The University has appointed a Data Protection Officer (“DPO”) to monitor internal compliance. This is an advisory role and is concerned with the University’s compliance with data protection legislation. The DPO shall:

- enable compliance with data protection legislation
- provide advice, assistance and recommendations in relation to data protection risks
- support and foster a data protection culture within the University
- help implement essential elements of data protection legislation, such as the principles of data processing, data subjects’ rights, data protection by design and by default, records of processing activities, security of processing and notification and communication of data breaches
- be the University’s point of contact with the Information Commissioner’s Office.

The DPO shall not determine the purposes of processing personal data, or the means by which any personal data processing activity is done.

**Notification of data* held and processed***

The University of Brighton undertakes to maintain an accurate and timely notification of its data processing activities with the Information Commissioner’s Office (ICO). The University is registered as a Data Controller and its registration number with the ICO is: **Z5395727**

**Responsibilities**

University Executive Board:

- shall ensure that the purposes and means of processing of personal data for which the University is data controller are determined in compliance with legislation.
- responsibility for ensuring implementation of, and compliance with, this policy will be in accordance with the University's line management structure.

All staff are responsible for:

- checking that any information that they provide to the University of Brighton in connection with their employment is accurate and up-to-date
• informing the University of Brighton of any changes to information already provided, e.g. 
  new address
• notifying the University of Brighton of any errors or necessary amendments. The University 
  of Brighton cannot be held responsible for any inaccuracies unless the staff member has 
  previously provided the University with the correct information

All staff (and any individual, organisation, or third party) that processes personal data on 
behalf of the University) is responsible for:
  • Ensuring that they comply with this policy and associated data protection, information 
    security, information management and information technology regulations, policies, 
    processes and procedures.
  • To undertake training as required

In order to embed best practice in the management of personal data across the University, the 
primary operational responsibility for the management of personal data lies with the relevant line 
managers. In order to provide clarity a number of data areas will be designated and the appropriate 
manager will be termed as the senior information owner for that area. In addition the University 
has established a number of additional roles to serve as supporting champions for the continuing 
enhancement of its data management.

The main responsibilities of the Senior Information Owners and those of the additional data 
champion roles are set out below.

**Senior Information Owners**

“Senior Information Owners" are accountable roles concerned with the management of 
all information within a specified data area. With regards personal data, they are 
responsible for:

• Departmental responsibility for compliance with relevent data protection legislation and 
  regulation in their data areas.
• Ensure that local processes and procedures are developed, implemented, followed and 
  regularly reviewed as they relate to the processing of personal data
• Ensuring that the DPO is involved properly, and in a timely manner, in all issues which relate 
  to the protection of personal data, and that the DPO is consulted promptly once a data 
  breach or another incident has occurred.
• The monitoring and mitigation of data protection risks, which could include ensuring 
  principle of data protection by design or default is applied with new or changing personal 
  data processing.
• Ensure that no individual is given access to personal data without having undertaken 
  appropriate training and read relevant policy and guidance
• Ensuring that staff who have access to the personal data within their remit are appropriately 
  briefed or trained on the processing of that data.
• Monitor sector or professional communications for data protection related issues or 
  benchmarking opportunities.
Departmental Information Security Representatives

Each department is required to nominate a person as Departmental Information Security Representatives to work alongside the above staff and to support compliance within the team/department. With regards to personal data their responsibilities are as follows:

- To work with the DPO on creating and maintaining an Information Asset Register
- Support and advise to colleagues, embedding data protection good practice/compliance culture
- Report areas of concern/risks to the DPO.
- Undertake regular reviews of data security in line with the Departmental Information Security Policy. Including regular review of permissions to ensure ongoing authorized access, ensure that equipment is disposed of appropriately and in accordance with policy.
- To regularly review and update retention schedules, in line with the appropriate legal basis for processing. Ensure data is deleted on a regular basis as per the retention schedules and report issues or areas of concern
- To be a departmental point of contact for issues such as, facilitating subject access requests, timely identification, investigation and mitigation for data breaches (being mindful of our legislative duty to report certain types of breaches within 72 hours)
- Ensure employees with university owned property e.g. computer equipment, books are returned
- Cascade training, communications and awareness as required

Data Stewards

This role has been created to support the wider assurance and enhancement of data management at the University under the remit of the Data Governance Group, and stewards are designated by that body. A separate Data Quality Framework, focusing on wider data management will be published. With regards to personal data the data stewards will be responsible for

- Ensuring and evidencing that the impact of personal data protection is explicitly and appropriately considered in the review and development of wider data management processes and policies.
- Alerting the DPO to any data protection concerns that emerge as a consequence of their data stewards activity.
- To undertake regular data protection training as necessary to support these responsibilities.

Student Responsibilities

Personal information

All students are responsible for:

- checking that information they provide to the University of Brighton in connection with their membership of the university is accurate and up-to-date.
- Advising the University of Brighton of any amendments to this information, e.g. changes of address. The University of Brighton cannot be held responsible for any errors unless the student has provided updated information as here requested.
In most cases updating your student record can be done via the ‘personal tab of studentcentral’ or via in person accessing Student Information Desk at your site of study.

**Students who process personal data**

Students who need to process personal data as a justifiable part of their studies or as part of employment with the University (whatever the level or mode) will be covered by the University of Brighton’s Data Protection Policy. They will be expected to observe the relevant guidelines issued by the University. Should they be processing on behalf of another organisation, whilst on placement for example, they will be bound by the Data Protection policies and provisions of that body as the Data Controller.

**Brighton and Sussex Medical School (BSMS)**

The Brighton and Sussex Medical School (BSMS) is a partnership between the Universities of Brighton and Sussex, which works with NHS organisations, in the delivery of education, training and research.

The responsibilities of both Universities for personal data are documented in the data sharing agreement and privacy notice here [https://www.bsms.ac.uk/about/privacy-policy.aspx](https://www.bsms.ac.uk/about/privacy-policy.aspx). See also the University of Sussex Data Protection Policy here: [https://www.sussex.ac.uk/about/website/privacy-and-cookies/privacy](https://www.sussex.ac.uk/about/website/privacy-and-cookies/privacy)

**Data Subject Rights - Staff and student data**

All staff, students and other users are entitled to

- access and obtain a copy of your data on request, this is known as a subject access request, see below;
- require the University to change incorrect or incomplete data;
- require the University to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data, in certain circumstances, for example, where the university is relying on its legitimate interests as the legal ground for processing; or for direct marketing purposes
- ask the University to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the University's legitimate grounds for processing data.
- withdraw your consent at any time, where we have requested and obtained your consent
- where our lawful basis is consent or performance of a contract we will allow portability of your data.

If you would like to exercise any of these rights, please contact the University’s Data Protection Officer, Rachel Page, Head of Data Compliance and Records Management, 01273 642010, dataprotection@brighton.ac.uk

**Subject Access request**

Staff, students and other users of the University of Brighton have the right to access any personal data that is being kept about them either on computer or in manual files.
Individuals wishing to exercise this right can follow the process here https://www.brighton.ac.uk/foi/requesting-information/index.aspx. (Note that requests must be accompanied by the appropriate ID).

There is no charge for this request but the University reserves the right to charge a ‘reasonable fee’ when a request is considered to be unfounded or excessive, or repetitive.

In accordance with the legislation, the University has 1 month with which to respond to a subject access request. Should there be a good reason for delay, this will be explained in writing to the data subject making the request.

Guidance for staff on how to respond or record a Subject Access Request can be found here https://staff.brighton.ac.uk/reg/legal/Pages/SAR.aspx

Students requiring replacement certificates and transcripts should follow the process here https://www.brighton.ac.uk/alumni/helping-you/index.aspx

Examination Scripts

Students may also make a request using the above procedure to obtain a copy of their exam scripts (written answers) once marks have been formally ratified and published. Students can request their mark, comments written by the examiner, minutes of any examination appeals panels. It does not give the right to copies of answers to exam questions. Further guidance on Exam Results is available from the ICO.

The right to complain to the ICO

If you are unsatisfied with the way the University has processed your personal data, or have any questions or concerns about your data please contact dataprotection@brighton.ac.uk, if we are not able to resolve the issue to your satisfaction, you have the right to apply to the Information Commissioner's Office (ICO). They can be contacted at https://ico.org.uk/

Data Breach

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data breaches could include, for example:

- Loss or theft of data or equipment (external hard drives, laptops) on which data is stored
- Inappropriate access controls allowing unauthorised use
- Contact details and financial details being accidentally emailed to inappropriate of incorrect recipients
- Equipment failure
- Unforeseen circumstances such as a fire or flood
- Hacking or phishing
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

Any breach of data may render the University liable to legal action by the ICO and may also amount to a disciplinary offence.
Data breach reporting

The University of Brighton will make every effort to avoid breaches of the Data Protection Act, and in particular the loss of personal data. All data breaches, whether accidental or not should be reported to the Head of Data Compliance and Records Management so that appropriate action can be taken, where possible to contain the breach or to advise any individuals likely to suffer distress or inconvenience as a result.

Any member of staff, student employed by the University or third party data processor, who becomes aware that they or another person has caused, or may have caused, an unintentional disclosure of personal data held by the University, or some other breach of the Data Protection Act by the University, is responsible for reporting it at the earliest possible point.

Further guidance is available on Staff Central, including the data breach form. Alternatively please contact dataprotection@brighton.ac.uk

International Data Transfers

Under Data Protection legislation a controller may not transfer personal data to a country outside the United Kingdom or to an international organisation unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

This is largely because individuals risk losing the protection of the UK data protection legislation if their personal data is transferred outside of the EEA. The most important distinctions are whether information will be held:

- within the UK
- within the EEA
- by a country on the European Commission’s approved list; or
- in another non-EEA country.

The University must ensure that adequate or equivalent controls are in place and all requirements of the legislation are complied with in respect of any transfer.

The DPO should be made aware of any transfer of personal data outside of the EEA.

Further information can be found at: https://staff.brighton.ac.uk/reg/legal/Pages/International_Data_Transfers.aspx

Sharing of Personal Data

Ensuring that personal data is shared appropriately and securely is vital to the successful operation and the reputation of the University, and for maintaining the trust of our employees, students and other stakeholders. In order to achieve this, the University shall

- Identify a clear objective, or set of objectives, for the sharing of personal data
- Identify a lawful basis in data protection legislation for the sharing of personal data
- Ensure that the sharing of personal data is necessary to achieve the identified objective(s). Anonymised or pseudonymised data shall be shared where the identification of data subjects is not required
- Share the minimum amount of personal data required to achieve the objective(s)
• Provide data subjects with privacy notices documenting who data is shared with and, where data subjects have a choice, seek consent for the sharing of their personal data
• Check the identity of the requester
• Agree Data Sharing Agreements or Contracts with the third party where more systematic data sharing is required.
• Enquiries/requests for disclosure from the Police should be directed to the DPO.

In all cases, if there is any doubt as to the validity of the enquirer or their enquiry, no disclosure should be made and the caller should be directed to the DPO.

A record of all non–routine disclosures will be retained.

Information for staff showing who might request personal information from the University either as a regular or ad hoc occurrence, and guidance on how to respond to requests is available here https://staff.brighton.ac.uk/reg/legal/Pages/Third-Party-Data-Disclosure.aspx

For those external to the University, requests for data can be made via: https://www.brighton.ac.uk/about-us/statistics-and-legal/requesting-information/index.aspx

Working with third parties who process data on our behalf

The University works with a number of third parties (data processors) that require access to the personal data of students and staff – this could include IT suppliers for the maintenance of systems, confirmation of academic awards to professional or statutory regulatory bodies, statutory reporting bodies such as Office for Students, UKRI or HESA. Many of these organisations are documented in the Privacy Notices, see: https://www.brighton.ac.uk/about-us/statistics-and-legal/privacy/index.aspx.

Where personal data is shared on a systematic basis or there is a large scale transfer of personal data, we will ensure that a written agreement (data sharing arrangement or contract) is in place, at a minimum this will conclude:

• The type or items, of personal data to be shared
• The source(s) of the personal data
• The objective(s) of the data sharing arrangement
• The lawful basis for sharing the personal data
• The individuals/groups that will have access to the personal data
• The methods by which the personal data will be transferred, including any controls for protecting the data from loss, destruction or unauthorised access
• The frequency with which the personal data will be shared
• Storage requirements for the personal data, including any controls for protecting the data from loss, destruction or unauthorised access
• The parties’ responsibilities for ensuring the accuracy of the personal data
• Retention and disposal requirements
• Arrangements for enabling data subjects to exercise their rights
• Processes and procedures for handling information security incidents.

The legislation specifies which terminology is to be included in such documents, so do check any documents with the DPO.
In addition, the University has template documents for this, please contact the Data Protection Officer.

Research and consultancy

Staff and, where relevant, students engaging in research will be covered by the University of Brighton's Data Protection notification. Provided that any research undertaken is not published in a way that would identify individuals or cause them damage or distress, data used for research purposes has certain exemptions from the terms of the Act. In practice, this means:

- there is no right of subject access to personal data where the information has been anonymised for research purposes and where the results do not identify individuals
- personal data may be held indefinitely
- there is no right of erasure (or, to be forgotten), as processing personal data for research is part of our public task. However where possible/practical we would give research participants the option to withdraw their data up to the point of anonymisation/aggregation/publication.

Despite the terms of these exemptions, the University of Brighton seeks to ensure that, wherever practically possible, data subjects are made fully aware of any research for which their personal data may be used. Researchers are required to keep their data secure and to guard against any accidental disclosure that might arise from direct or indirect reference to individuals in any research report.

Consultancy undertaken for and on behalf of an organisation other than the University of Brighton may be subject to the Data Protection Policy and provisions of that organisation as well as those of the University, depending upon the nature of the agreement or contract. Please refer any queries to the Director of Legal Services.

Social Media

Whilst the open and accessible nature of social media networks can be helpful, by its very nature, social media enables and encourages users to share personal data, including for example photographs. If you are using social media, you should never publish colleagues’ or students personal information, and ensure that any processing is in line with this Data Protection Policy and the Data Protection Act 2018.

All uploads, storage and communications must be lawful and fair. Staff intending to use a social media account must ensure that all parties know what type of information they are expected to share, for what purpose and who will have access to it. Staff should be familiar with privacy settings and ensure that these are appropriate for both content and intended audience. Staff are also responsible for ensuring appropriate informed consents are in place.

Staff are responsible for ensuring that passwords and other access controls for University social media accounts are of adequate strength and kept secure. Do not use the same password for accessing both University systems and a social media site. Passwords should be changed regularly and under no circumstances, should passwords be shared.

Staff should ensure that any devices that have social media login details stored on them are set to lock or log out automatically after each use and if any devices which contain login details are lost
or stolen, staff should change the passwords of all social media accounts that the device was connected with, and let other managers of the accounts know.

You should be aware that social media sites are used extensively by malicious individuals to gain information about you or others in order to assist with their activities or impersonate you. Take care with your postings so that someone is unable to work out information about you – where you live, work, telephone numbers. Only accept invitations from people you really know, and if you are not sure of someone's identity then ask them directly to confirm. Don’t click on unsolicited links - these may install malicious software or spyware on your computer or device.

You should also be aware that applications running on social media sites may send your profile data to third parties over which you have no control – so do check the privacy content.

Staff should ensure they adhere to the Social Media Policy and Social media guidelines.pdf.

CCTV

The University operates a CCTV monitoring system around its properties. The function of this system is to assist in the detection and deterrence of crime and to assist the Police and civil authorities in the event of a major emergency. The system will be operated in such a way as to safeguard individuals' right to privacy.

All CCTV images have ownership and copyright vested in the University of Brighton. Cameras will be mounted in public view and signs will be displayed warning of their presence and the purposes of their operation. Recorded images will normally be preserved for a period to be determined in accordance with the University Records Retention Schedules. After this period, if they are not needed for evidential purposes, the recording media will be re-used. If required for evidential purposes, they will be retained for as long as is necessary to the prosecution of the case.

Retention of data

Student records

In general, detailed information about students will be kept in the relevant school for a maximum of two years after they leave the University of Brighton. This will include:

- name and most recently notified address
- academic achievements, including marks for coursework
- copies of any reference written

After this period, information will be destroyed. Information on what was studied by the student, what s/he achieved and any periods of intercalation will be available from Academic Services. These records are kept indefinitely as part of our public task to confer academic awards, see also https://www.brighton.ac.uk/alumni/helping-you/index.aspx.

Please refer to the Privacy Notices for links to the relevant retention schedule.

All personal records will be disposed of securely to ensure there is no accidental disclosure to third parties.

Following completion of studies and to enable ongoing communication/interaction, student details are passed to the university’s Alumni Association (run by the Philanthropy and Alumni Engagement department). This means the primary point of contact for former students will be the Alumni
Association, in terms of updating details or seeking advice/support as a graduate. More information about the Alumni Association and what it offers former students can be found by visiting www.brighton.ac.uk/alumni

Staff records

In general, local departmental records will be retained for up to a year after someone leaves. Central records, held by HR will be kept for six years after s/he has left the University. Some records, however, will be kept for much longer. This will include material necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment.

Please refer to the Privacy Notices for links to the relevant retention schedule.

All personal records will be disposed of securely to ensure there is no accidental disclosure to third parties.

Conclusion

Compliance with the DPA is the responsibility of all members of the University of Brighton. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to University of Brighton facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be directed to the Head of Data Compliance and Records Management

Policy Review and Maintenance

This policy shall be reviewed DPO annually or whenever there is a significant change in legislation, strategy or organization. Major changes shall be approved by the IT Governance Board.

Related Policies

UoB Information Security Policy
UoB Departmental Information Security Policy
UoB IT Regulations

Related Guidance

Data Protection information on staff central

Information Services also have information on safe computing: https://staff.brighton.ac.uk/is/computing/Pages/Safe-computing.aspx
Appendix 1 Glossary of Data Protection Terms

Data: in the context of the University of Brighton, information which is processed automatically/recorded with that intention or is recorded as part of a relevant filing system/with that intention.

Data Breach: A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data Controller: the person/people who determine(s) the purposes for which, and the manner in which, personal information is to be processed and whose duty it is to ensure that the Data Protection Principles are applied. In the context of this institution, the Data Controller is the University of Brighton.

Data Processor: a person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Protection Act 2018 (DPA): Sets out the data protection framework in the UK, alongside the GDPR. It contains four separate data protection regimes:
- Part 2 Chapter 2 (GDPR): supplements and tailors the GDPR;
- Part 2 Chapter 3 (applied GDPR): extends a modified GDPR to some other (rare) cases;
- Part 3: sets out a separate regime for law enforcement authorities; and
- Part 4: sets out a separate regime for the three intelligence services.

Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data. See https://staff.brighton.ac.uk/reg/legal/Pages/Data-Protection-by-Design.aspx

Data Protection Officer: Under Data Protection Act 2018, organisations are required to appoint a data protection officer (DPO) to be responsible for monitoring compliance with the Regulation, providing information and advice, and liaising with the supervisory authority. At the University of Brighton, this is Rachel Page Head of Data Compliance and Records Management. r.j.page@brighton.ac.uk, ext 2010, based in 802 Cockcroft.

Data subject (individual) means an identifiable natural person “who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier.

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data. See https://staff.brighton.ac.uk/reg/legal/Pages/SAR.aspx

General Data Protection Regulation 2018 (GDPR) The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

Inaccurate Data: data which is incorrect or misleading as to a matter of fact.

Notification: entry on the public register maintained by the Information Commissioner’s Office showing types and range of information being processed by the university. The Universitys registration number is: Z5395727
Personal Data: “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, 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.

Processing: obtaining, recording or holding information, or carrying out any operation or set of operations on the information. This includes organising, adapting, or altering the information, disclosing and deleting.

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.

Special Category Data: information as to the individual’s

- racial or ethnic origin
- political beliefs
- religious beliefs or beliefs of a similar nature
- trade union membership
- Genetics
- Biometrics (where used for ID purposes
- physical or mental health or condition
- sex life or sexual orientation

The Data Protection rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. However, there are separate safeguards for the relating to criminal convictions and offences, or related security measures, set out in Article 10.

Further Information:


Appendix 2 Data Protection Principles

The data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.


Appendix 3 Use of Staff Images

1. Introduction

1.1 This policy has been written to ensure that the University of Brighton complies with legal requirements in the use of staff images.

1.2 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the University of Brighton

2. Publication of staff images by the University of Brighton

2.1 When staff join the University they are required to upload an identification photo as part of their application for a UniCard. This photograph is used for a variety of identification and authentication purposes only.

2.2 Specific guidance on how the University uses such photos can be found at https://staff.brighton.ac.uk/is/Published%20Documents/UniCard-photo-policy.pdf

2.3 Photos will not be shared with third parties, unless for exceptional purposes.

3. Photograph - Online Image Publishing

3.1 By default the photo you submit for your Unicard, will not be published on staff central. Staff can ‘opt in’ to consent to their photograph being viewed – this can be done via MyInfo. Staff are invited to ‘opt in’ to one or both of two choices:

i. Consent to the University using their image for internal communication (‘non-public’) purposes and or publicity purposes (see 4 below). ¹

ii. Consent to the University using their image for external communication (‘public’) purposes and or publicity purposes (see 5 below). ¹

¹ When staff central is upgraded to O365, there will no longer be an option to feed staff photos on staff central.
iii. If you select neither option, your identification photo will not be viewable on staff central (unless a photo has been manually added to a page). If you have not opted in then a basic grey silhouette will display instead.

3.2 Once consent has been given, it is not required that an individual be contacted for specific instances. Individuals may however be contacted to enquire about the suitability of an image.

3.3 Staff may choose to opt in or opt out at any time.

3.4 Staff photos will not be automatically published on student central, though staff are encouraged to add photos to welcome pages and contact areas.

3.5 If you want your photo to be visible to staff and students whilst they are working in Office 365, see instructions here.

4 Some Academic Schools include photos of their students/staff on their individual or internal web pages, within the University website, or on noticeboards – you will be asked to give specific consent for this

4. Consent to the University using their image for internal communication (‘non-public’) purposes and or publicity purposes

4.1 In this context ‘non-public’ refers to areas of Staffcentral that can only be accessed by means of a login and University of Brighton computer account.

4.2 Having a photo visible on staff central, allows the University to improve internal communications, and facilitate working across departments and campuses.

4.3 Examples of this are – but not restricted to:

i. The use of staff profile photos on the internal ‘staff central’ intranet contacts directory.

ii. The use of staff profile photos appear on any committee pages or team contact pages where you are a listed member, so colleagues can see who they are working with or who to contact for specific issues.

4.4 For photographs used to support internal communications work on any communication channel (for example staff news stories on the intranet, internal social media channels), individuals will be contacted for a suitable photo or to arrange a photograph to be taken.

5. Consent to the University using their image for external communication (‘public’) purposes and or publicity purposes

5.1 ‘External’ or ‘public’ purposes in this context means the display of staff photographs on the University website or any part of Staffcentral visible by members of the public without the need to login.

5.2 Individuals will usually be contacted for a suitable photo or to arrange a photograph to be taken. (to note, selecting option described in 3.1 ii will mean your photo appears on public areas of staff central).

5.3 Examples of this are – but not restricted to:

i. The use of staff photographs to accompany individual contact details on the university website or public areas of staff central

ii. The use of staff photographs to illustrate external communications work on any communication channel (for example news stories on the university website, press releases or social media channels) or University publications such as Prospectus

iii. The display of staff photos on walls, for example in a school foyer.
5.4 Certain types of contact details for senior staff, including photos will be available via the university website, this includes names and images of the University Board of Governors, University Executive board, Heads of Schools, and Directors of Professional services. In most cases a separate photograph will be taken.

5.5 We have produced separate guidance for the use of images to be used for publicity purposes Guidance for images (photographic and video) intended for publicity purposes.

6. **Suitability of images**

6.1 Staff photos must not potentially offend others, or show incriminating or embarrassing behaviour. Photos must not undermine the University’s positive reputation and values. Guidance on what makes a suitable photo can be found at https://staff.brighton.ac.uk/is/unicard/Pages/student_photos.aspx

6.2 Any staff member may be requested to remove a personal photo with a more suitable image.

If you are a student or staff with concerns about your data being used in this way, please contact dataprotection@brighton.ac.uk

**Appendix 4 Unicard**

All students and staff of the University community are expected to have a UniCard. Personal information (which includes an image) held on the database will be treated confidentially, and will only be used for the purposes of card administration.

As part of your application for a UniCard you are required to upload an identification photo, information on the use of photographs can be found at: https://staff.brighton.ac.uk/is/unicard/Pages/student_photos.aspx

This photograph is used for a variety of identification and authentication purposes only. The UniCard enables access to a range of facilities and services and as such data is extracted and shared with other systems to enable members of staff, students and associates to access University facilities and services – this includes identification; access to buildings or rooms; borrowing items from the Library; to use the bus service; to use sports facilities, cashless purchasing, and authentication for printing and copying.

Data will be processed in accordance with relevant legislation and, specifically, in accordance with the provisions of the Regulation of Investigatory Powers Act (2000).

Unless specifically requested, for legislative or academic reasons, personal UniCard data will be deleted from the system 90 days after the user of the UniCard is no longer employed by the university or is not attending any course – data shared with other systems will be deleted in accordance with that systems retention guidelines.

The University may share information held on UniCard and the Print system with other departments of the University and / or appointed agents: to provide users with the service applied for; to help resolve a complaint, for analysis and / or Management Information; or: for purposes of fraud prevention, audit or debt collection; other cardholders, but only where it is considered necessary for resolution of fraud or dispute and for the investigation of crime or in connection with disciplinary investigations.
Konica Minolta MFDs

The University uses Konica Minolta MFDs for printing, copying and scanning. Access to these facilities is enabled by the UniCard, and administered by Information Services.

- Records will be treated confidentially will only be used for the purposes of finance, administration and support of printing services.
- Where appropriate, data (printing statistics) will be extracted and shared with departments to enable selected members of staff to review departmental printing usage.
- All documents are deleted once they have been printed by the MDF printer. Documents not printed are deleted after 72 hours.
- All users’ individual printing records (a record of the printing, not the actual file) are retained for five years in line with legal requirements associated with financial transactions i.e. departments and students are charged for printing. After the statutory period, the transactions are deleted.
- Printing accounts are deleted five years after a student or staff has have left the University.

Access Control Records

Access to buildings is facilitated by the UniCard, and administered by the Estates and Facilities Management Department. Records relating to an individual’s use of the UniCard to gain access to University premises will not routinely be divulged to internal or external parties. This information may lawfully be disclosed, however, in connection with a disciplinary or criminal investigation or because of health and safety concerns. Such disclosure is subject to the specific authorisation of a member of the University Executive Board.

Access control data will normally be retained on the system for 90 days only, and will then be archived. After 180 days the records will be deleted.

Please see UniCard Webpages for further details of the terms and conditions for UniCard.