# Data protection policy

Birkbeck, University of London is committed to protecting the rights and freedoms of all individuals in relation to their personal data. Birkbeck needs to comply with the Data Protection Act and the General Data Protection Regulations (GDPR). This policy sets out the obligations of staff and students in this respect.

Birkbeck needs to collect and keep certain types of information about the people with whom it deals. This includes students, staff, alumni, contractors, users of our services and others. Birkbeck needs to process this information for a number of reasons, for example to record the academic progress of students, to recruit and pay staff and to comply with statutory obligations such as equality and diversity and health and safety.

This policy applies to all personal data handled by Birkbeck staff, students and other authorised individuals, in all formats including paper and electronic files, on computers and mobile devices and regardless of who owns the device on which it is stored.

**1. Definitions**

1.1 Processing

The DPA and GDPR refer to "processing" of data. "Processing" is any action taken in relation to the data, including obtaining, recording, storing, using, sharing, disclosing, erasing or destroying it.

1.2 Personal data

Personal data is data which relates to a living individual who can be identified from the data and other available information.

1.3 Special category data

Special category data is more sensitive personal data, requiring greater protection. This includes data on

- race,
- ethnic origin,
- political opinions,
- religious beliefs or beliefs of a similar nature,
- trade union membership,
- genetics,
- biometrics used for ID purposes,
- health,
- sex life and sexual orientation,

Staff working in certain research areas with human participants, or in certain roles including Disability Advice and HR, will have regular access to special category data. Others are likely to do so rarely if at all.

1.4 Data about criminal convictions and offences

Data about criminal convictions or offences also needs greater protection and must be handled similarly to special category data.

1.5 Confidential data

Confidential data is data given in confidence, or with an agreement for it to be kept confidential. Some confidential data will also be special category data and will come within the terms of this policy.

1.6 Research data

Some staff will handle research data, comprising materials collected or created for the purposes of analysis to generate original research results. When research data contains personal data and/or special category data, the provisions of this policy apply. Please see section 11 and http://www.bbk.ac.uk/committees/research-integrity for more information on how to deal with research data.

**2. Responsibilities of staff, students and other authorised individuals**

2.1 Data Protection Officer

The College Data Protection Officer (DPO) is responsible for advising on and facilitating compliance with GDPR and data protection legislation. The DPO will advise on all aspects of data protection and will co-ordinate the production and maintenance of documentation required to demonstrate compliance.

2.2 Data Custodians

While all staff are responsible for protecting privacy and personal data as set out below, the College has designated certain lead, supervisory and senior staff as Data Custodians.

Data Custodians are responsible for overseeing data protection compliance in specific instances in which personal data is collected and processed in individual departments, teams and systems, liaising with the DPO to ensure that this policy is adhered to, staff are aware of and able to adhere to its provisions, and that required documentation for processing the data is in place and kept up to date.

For research data, the academic supervisor, Principal Investigator or Head of Department will be the Data Custodian.

2.3 Responsibilities for all

All staff, students and other authorised individuals must:

- Be aware that individuals have the rights in relation to their personal data described in 5 and 13 below. Staff should take care to ensure comments or data about students and prospective students meet the expectations of GDPR, in relation to relevance, transparency and accuracy. This applies to emails and notes as well as structured records
- Immediately report to their line manager and the DPO if they find any lost or discarded data which may contain personal data, including papers and memory sticks
- Immediately report to their line manager and the DPO if they believe personal data has been accidentally lost, stolen, inadvertently disclosed, for example if their laptop, phone or memory stick is lost or stolen, or made inaccessible, for example if data is maliciously encrypted.
- Not disclose personal information orally, in writing, electronically, or by any other means, accidentally or otherwise, to any unauthorised third party.

- Keep personal data securely. There is more information on how to do this at http://www.bbk.ac.uk/privacy
- Ensure all personal data they provide to Birkbeck is accurate
- Notify Birkbeck promptly of any changes in their personal data
- Only collect and process personal data of others for approved work or study related purposes. If in doubt, contact the DPO

2.4 Staff, students and other individuals with access to personal data must

- Ensure that they only process personal data in accordance with the GDPR principles. The best way to do this is through familiarisation with this policy and related guidelines published on our website www.bbk.ac.uk/privacy. Key points for compliance include:
    - Data is processed lawfully, fairly and in a transparent manner so that individuals are informed and aware and where necessary have given explicit consent
    - Data is processed only as set out in the relevant privacy notice(s). These are available at www.bbk.ac.uk/privacy.
    - Data is collected only for the specified lawful purpose and not processed for any other purpose.
    - Processing is limited to what is adequate and necessary for the specified lawful purpose.
    - Personal data is accurate and where necessary kept up to date.
    - Personal data is not kept for longer than necessary for the specified lawful purpose.
    - Personal data is kept secure and protected against unauthorised disclosure and processing and accidental loss, destruction or damage.
- Ensure they are familiar with this policy and the guidelines at www.bbk.ac.uk/privacy
- Ensure they are familiar with the Birkbeck Computing Regulations and related policies (see http://www.bbk.ac.uk/its/regulations)
- Seek advice from the DPO whenever a new form of processing is to be introduced, or if any data protection related concerns arise.

**3. Data security**

3.1 Keeping personal data properly secure is key in complying with GDPR. All staff are responsible for ensuring that if they keep personal data it is kept securely and not disclosed, either orally, in writing or electronically, to any unauthorised third party.

3.2 Staff should ensure that personal data on computer and phone displays, and on paperwork in offices, is only viewable by authorised staff.

3.3 Personal data held on phones, laptops and other portable devices must be password protected or where appropriate encrypted.

3.4 Personal data in paper form or on discs, external drives or memory sticks must be kept in a secure locked location.

3.5 Staff should take special care to ensure security whenever data is transferred from one place to another, using password protection and encryption as appropriate.

3.6 Staff working away from the office should ensure that data is processed and stored securely. Please see the remote device security policy at http://www.bbk.ac.uk/its/regulations

3.7 Please see http://www.bbk.ac.uk/privacy and http://www.bbk.ac.uk/its/regulations for more information and if in doubt consult the DPO.

## 4. Lawful basis for processing

4.1 The GDPR require Birkbeck to identify the lawful basis for processing each type of information. The lawful basis will vary according to the type of information, and is likely to be one of the following:

- The individual has given clear consent for their data to be processed for a specific purpose
- The processing is necessary to fulfil a contract with the individual
- The processing is necessary to enable Birkbeck to comply with the law
- The processing is necessary for Birkbeck to perform a task in the public interest, related to the Objects of Birkbeck as set out in its Charter: to provide education and means for research in academic disciplines
- The processing is necessary for Birkbeck's legitimate interests, and it has been established that the need to protect individuals' personal data does not override those interests

4.2 Special category data and data on criminal convictions and offences can only be processed if additional conditions are met.

4.3 Special category data can only be processed if there is a lawful basis for processing (see 4.1) and additional conditions are met, such as

- The individual has given explicit consent
- Processing is necessary to comply with the law and in the interests of the individual
- Processing is necessary to protect the vital interests of the individual and the individual is incapable of giving consent
- Processing related to personal data which have been made public by the data subject

Please consult the DPO for advice about processing special category data.

4.4 Data about criminal convictions and offences can only be processed if there is specific legal authorisation to do so. Please contact the DPO for advice about processing criminal conviction and offence data.

## 5. Rights of individuals

5.1 GDPR gives individuals rights in relation to the processing of their personal data:

- Right to be informed
- Right to access data
- Right to rectification
- Right to erasure
- Right to request restriction of processing
- Right to data portability
- Right to object to processing

Please see 13 for more details.

5.2 Information for individuals on how to request access, rectification, erasure, restriction of personal data and how to object to processing of personal data will be available at www.bbk.ac.uk/privacy.

## 6. Documentation

6.1 For every instance in which personal data is collected and processed, Birkbeck will create and maintain a record of the processing activity.

6.2 The record will include:

- A description of the individuals and the data being collected and processed
- The privacy notice, which must also be provided to individuals at the time the data is collected, and which includes:
    - Birkbeck's name and contact details,
    - the data that will be collected,
    - the purpose of processing
    - the lawful basis for processing (see 4 above),
    - the legitimate interest for processing if applicable
    - the period that the data will be retained for,
    - the rights of the individual in relation to the data
    - who the data will be shared with.
    - the source of the data
- Records of consent if applicable
- The location of the data
- Data Protection Impact Assessment Reports, if appropriate
- A description of the organisations that the data will be shared with, and copies of contracts
- Details of any transfer to other countries, including the safeguards in place to protect the data
- A description of the measures in place to ensure the security of the data
- Retention schedules
- Records of personal data breaches

6.3 Data Protection Impact Assessments

For instances when there is an increased risk to individuals' privacy rights and freedoms, including new and major projects and use of new technologies, the DPO and Data Custodian should conduct a Data Protection Impact Assessment (DPIA). More information is available on www.bbk.ac.uk/privacy.

There is a screening checklist to assess whether a DPIA is necessary. This should be applied in every instance in which personal data is collected and processed, including existing operations.

If a DPIA identifies a high risk that cannot be mitigated, the DPO should consult the Information Commissioner's Office.

**7. Retention and disposal**

7.1 The retention schedule for personal data will vary according to the type of data and the purpose of processing. In some cases the retention schedule will be governed by legal requirements.

7.2 The Data Custodian, advised by the DPO, is responsible for ensuring data is destroyed at the end of the retention period.

7.3 Paper files will normally be destroyed by shredding or use of the confidential waste disposal service

7.4 Electronic files will normally be deleted.

7.5 Any computers, phones or portable devices that are to be sold or scrapped must have had all personal data stored in them completely destroyed. Data Custodians and the DPO should

consider whether the devices themselves should be destroyed if it is not possible to be certain that the data in them has been destroyed.

**8. Personal data breaches**

8.1 Staff and students should report any actual or suspected loss or unauthorised disclosure of personal data without delay to their line manager if applicable and to the DPO.

8.2 The DPO, in consultation with the Data Custodian and relevant senior staff, will determine whether there is a need to report the breach to the Information Commissioner's Office. If it is necessary to report the breach this will be done within 72 hours of becoming aware of the breach, wherever feasible.

8.3 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Data Custodian will also inform those individuals without undue delay.

8.4 The Data Custodian and DPO will keep a record of any personal data breaches, regardless of whether they were notified to the Information Commissioner's Office.

**9. International/EU transfers**

9.1 Any transfer of personal data to third parties located in other countries will be strictly in relation to the delivery of Birkbeck's core services, including transfer to agents and partner institutions abroad, data sharing for the provision of IT services and hosting of data overseas. All instances of overseas transfers of personal data must be subject to appropriate technical safeguards and contractual provisions incorporating appropriate assurances to ensure the security of the data is fully compliant with the UK's data protection legislation.

**10. Children's data**

10.1 Children need particular protection when their data is being collected and processed because they may be less aware of the risks involved. Staff, students and others who intend to work with children's personal data should consult the DPO for advice. Privacy notices should be written in clear and age appropriate language and processes should be designed to be fair and to protect the data subjects.

**11. Research**

11.1 Before starting any research which will involve collecting and processing personal data, the researcher and their academic supervisor, Principal Investigator or Head of Department as appropriate must give proper consideration to this policy and the guidance on the www.bbk.ac.uk/privacy. Proposed research involving human participants will also require ethical approval through the Procedures for Ethical Review. Please consult http://www.bbk.ac.uk/committees/research-integrity.

**12. Implications of breaching this policy**

12.1 It is a condition of employment for staff, and enrolment for students, that staff and students comply with this policy. Any breach of this policy will be considered to be a disciplinary matter and may lead to disciplinary action. Serious breaches may also result in Birkbeck or the member of staff or student concerned being held liable in law.

**13. Delivering the rights of individuals**

13.1 Right to be informed

Individuals have a right to be informed about the collection and use of their personal data. This will be done through a Privacy Notice, provided to individuals at the time the data is collected, which will set out

- Birkbeck's name and contact details,
- the data that will be collected,
- the purpose of processing
- the lawful basis for processing,
- the legitimate interest for processing if applicable
- the period that the data will be retained for,
- the rights of the individual in relation to the data
- who the data will be shared with.
- the source of the data

13.2 Right to access data

Individuals have the right to access their own personal data and to be aware of and verify the lawfulness of the processing. This includes the right to obtain confirmation that the data is being processed, access to the data and access to the information in the Privacy Notice.

Birkbeck will provide this information on request:

- free of charge, unless the request is repetitive or excessive, in which case a fee will be charged based on the administrative cost of providing the information.
- within one month of receipt of the request, unless requests are complex or numerous. In such cases, there may be an extension of up to two months and the individual will be informed and reasons given within a month of the request
- normally in a secure electronic format accessible to the individual, unless there are reasons to provide the information in another format

Birkbeck will take reasonable steps to verify the requestor's identity

When requests are made for large quantities of information, Birkbeck will ask the individual to specify the information required

Birkbeck may refuse to provide information if a request is manifestly unfounded or excessive, giving reasons for refusal. Individuals may complain to the Information Commissioner's Office if they are not satisfied with the refusal of a request.

13.3 Right to rectification

Individuals have a right to have inaccurate data rectified and incomplete data completed.

Birkbeck will consider and action requests for rectification,

- free of charge, unless the request is repetitive or excessive, in which case a fee will be charged based on the administrative cost of locating and rectifying the information.
- within one month of receipt of the request, unless requests are complex or numerous. In such cases, there may be an extension of up to two months and the individual will be informed and reasons given within a month of the request

Birkbeck will take reasonable steps to verify the requestor's identity.

When requests are made for large quantities of information, Birkbeck will ask the individual to specify the information required.

Birkbeck may refuse to rectify information if a request is manifestly unfounded or excessive, giving reasons for refusal. Individuals may complain to the Information Commissioner's Office if they are not satisfied with the refusal of a request.

If the data that has been rectified is shared with other organisations, Birkbeck will take action to inform these organisations and provide them with the rectified data.

13.4 Right to erasure

Individuals have a right to have personal data erased, if

- The data is no longer necessary for the purpose it was collected for
- The data was collected with the individual's consent to process and the individual has withdrawn consent
- The data was collected on the basis of Birkbeck's legitimate interests, the individual objects to processing and there is no overriding legitimate interest to continue processing
- The data is being processed for direct marketing purposes and the individual objects to that processing
- The data is being processed unlawfully
- Birkbeck is legally obliged to erase the data

The right to erasure does not apply if processing is necessary

- To exercise the rights of freedom of expression and information
- To comply with a legal obligation
- The processing is necessary for Birkbeck to perform a task in the public interest (see 4.1 above)
- For archiving or research purposes in the public interest
- For the establishment, exercise or defence of legal claims

Birkbeck will consider and apply requests for erasure,

- free of charge, unless the request is repetitive or excessive, in which case a fee will be charged based on the administrative cost of locating and rectifying the information.
- within one month of receipt of the request, unless requests are complex or numerous. In such cases, there may be an extension of up to two months and the individual will be informed and reasons given within a month of the request

Birkbeck will take reasonable steps to verify the requestor's identity.

Birkbeck may refuse to erase information if a request is manifestly unfounded or excessive, giving reasons for refusal. Individuals may complain to the Information Commissioner's Office if they are not satisfied with the refusal of a request.

If the data that has been erased is shared with other organisations, Birkbeck will take action to inform these organisations and ask them to erase the data

13.5 Right to request restriction

Individuals have the right to request restriction or suppression of their personal data if

- They are also asking for data to be rectified or erased.
- The data has been unlawfully processed
- Birkbeck no longer needs the data but the individual needs it to be kept in relation to a legal claim

- The data was collected on the basis of Birkbeck's legitimate interests, the individual has objected to processing and Birkbeck is establishing whether there is an overriding legitimate interest to continue processing

Birkbeck will consider and apply requests for restriction,

- free of charge, unless the request is repetitive or excessive, in which case a fee will be charged based on the administrative cost of locating and restricting the information.
- within one month of receipt of the request, unless requests are complex or numerous. In such cases, there may be an extension of up to two months and the individual will be informed and reasons given within a month of the request

Birkbeck will take reasonable steps to verify the requestor's identity.

Birkbeck may refuse to restrict information if a request is manifestly unfounded or excessive, giving reasons for refusal. Individuals may complain to the Information Commissioner's Office if they are not satisfied with the refusal of a request.

If the data that has been restricted is shared with other organisations, Birkbeck will take action to inform these organisations and ask them to restrict the data.

Data may be restricted by making it unavailable to users and/or temporarily removing it from websites. Date must not be processed or changed while the restriction is in place.

If a data restriction is lifted, for example because it has been rectified, Birkbeck will inform the individual and other organisations with whom the data is shared.

13.6 Right to data portability

In some circumstances individuals have a right to obtain and re-use their personal data for their own purposes across different services. This only applies where processing is based on the individual's consent or the performance of a contract, and when processing is carried out by automated means.

13.7 Right to object

Individuals have the right to object to the following:

- Processing based on the basis of legitimate interests or the performance of a task in the public interest
- Direct marketing and profiling
- Processing for the purposes of research and statistics

Birkbeck will consider whether there are compelling legitimate grounds for the processing which override the interests rights and freedoms of the individual, or

whether processing is necessary for establishment exercise or defence or legal claims. If there are no such grounds, it will stop processing the data

Individuals have rights in relation to automated decision making and profiling. Birkbeck does not currently process, or plan to process, data in this way. We will revisit this section of the policy if appropriate in future.

**14. Personal data in the public domain**

14.1 Birkbeck holds certain information about staff and students in the public domain. This information will be publicly available, normally through our website, and will be disclosed to third parties without referral to the data subject.

14.2 Birkbeck's practice is to make the following data available freely unless individuals have objected

- Names of senior officers and Governors
- Minutes of Governors and committee meetings, including names of individuals present, unless the minutes record personal or commercially sensitive data

May 2018