Data Protection Policy

PLEASE NOTE: A new Data Protection Policy, compliant with the requirements of the Data Protection Act 2018 and the European General Data Protection Regulation (GDPR), is currently undergoing the approval process at the University and will shortly replace this policy.

Introduction
The University of Birmingham ("the University") needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It also needs to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the University must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998 ("the Act").

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Anyone who processed data on behalf of the University, including staff (including honorary staff), students, volunteers, contractors or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the University has developed the Data Protection Policy.

A glossary of terms and list of useful resources is attached to this Policy.

Status of the Policy

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 from time to time. **Any failures to follow the policy can therefore result in disciplinary proceedings.**

Any member of the University, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Data Protection Officer initially. If the matter is not resolved satisfactorily it could be raised as a formal grievance or complaint.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the University in connection with their employment is accurate and up to date.
- Informing the University of any changes to information, which they have provided, eg changes of address.
- Informing the University of any errors or changes in staff information. The University cannot be held responsible for any such errors unless the staff member has informed the University of them.

If and when, as part of their responsibilities, staff collect information about other people, (eg about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff (Appendix 1).

Data Security

All staff and students are responsible for ensuring that:

- Any personal data, which they process, is kept securely in accordance with the University's Information Security Policy;
- Personal information is not disclosed accidentally or otherwise to any unauthorised third party.

Student Obligations

Students must ensure that all personal data provided to the University is accurate and up to date. They must ensure that changes of address etc are updated on the student registration system.

Students may, as part of a project, process personal data. If they do so they must comply with the University's Data Protection Policy and Information Security Policy.

Rights to Access Information

Staff, students and other users of the University have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact Legal Services, in writing.

The University will make a charge of £10 on each occasion that access is requested.

The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days.

Subject Consent

In many cases, the University processes personal data with the consent of the individual. If the data is sensitive, express consent must almost always be obtained. Agreement to the University processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

All prospective staff and students will be asked to consent to their data being processed when an offer of employment or a course place is made. A refusal to sign such a form without good reason may result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process sensitive personal information. This may be to ensure the University is a safe place for everyone, or to operate other University policies, such as the sick pay policy or equality policies. The University will also ask for information about particular health needs, such as allergies to particular forms of medication, or any health conditions or disabilities. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the University to process this information.

The Data Controller and the Data Protection Officer

The University as a body corporate is the data controller under the Act, and the University Council is therefore ultimately responsible for implementation. However, the Data Protection Officer will deal with day to day matters.

The University has designated Mrs CM Pike OBE (Director of Legal Services) to act as Data Protection Officer. Any query relating to the implementation within the University of the Act and Subject Access Requests under section 7 of the Act should be referred to Legal Services.

Examination Marks

Students will be entitled to information about their marks for both coursework and examinations as part of their tutorial support. This is within the provisions of the Act relating to the release of data. However, this may take longer than other information to provide.

Retention of Data

The University will keep some forms of information for longer than others.

Data on students, including any information on health, race or disciplinary matters, will be destroyed after 10 years but a skeletal record will be retained to include a full transcript of academic achievements.

The University will need to keep central personnel records indefinitely. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

Research data must be retained in accordance with the Code of Practice for Research.

Compliance

Compliance with the Act is the responsibility of all members of the University. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to University facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

This policy was approved by the University's Council on 17 December 2007 and updated in May 2017 and takes immediate effect.

Data Protection Act 1998

Guidelines for Staff – Appendix 1

1. Members of staff will process personal data on a regular basis. The University will ensure that staff and students give their consent to processing, or that another condition for processing applies, and are notified of the categories of processing, as required by the Act.
2. Information about an individual's physical or mental health; sexual life; political or religious views; trade union membership; ethnicity or race; the commission of criminal offences and court proceedings dealing with criminal offences is sensitive and can normally only be collected and processed with their express consent.
3. Members of staff have a duty to make sure that they comply with the data protection principles, which are set out in the University Data Protection Policy. In particular, staff must ensure that records are:
    - accurate;
    - up-to-date;
    - fair;
    - kept and disposed of safely, and in accordance with the University policy.
4. Individual members of staff are responsible for ensuring that all data they are holding is kept securely.
5. Members of staff must not disclose personal data, unless for normal academic, administrative or pastoral purposes, without authorisation or agreement from the Data Protection Officer, or in line with the University policy.
6. Members of staff must complete University registrations forms in respect of all databases holding personal data before commencing processing of the data. The University may need to amend its registration with the Office of the Information Commissioner. Forms and advice are available from Legal Services on extension 43916 or https://intranet.birmingham.ac.uk/legal-services/index.aspx .
7. Before processing any personal data, all staff should consider the checklist.
8. All staff should either complete online data protection training through Canvas or attend an open training session through POD, and make themselves aware of the Data Protection Toolkit and other resources on the Legal Services website.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual or data subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that one of the other conditions for processing data applies?
- In respect of databases containing personal data, have you notified Legal Services that you intend to hold the data and registered the database?
- How long do you need to keep the data for, and what is the mechanism for review/destruction?

Glossary of Terms

Data

Any information held by the University for the purposes of University business.

Personal Data

Information about a living person. This information is protected by the Act.

Data Subject

The person about whom the data are held.

Sensitive Data

The Act introduces categories of sensitive personal data, namely, personal data consisting of information as to:

a. the racial or ethnic origin of the data subject,
b. their political opinions,
c. their religious beliefs or other beliefs of a similar nature,
d. whether they are a member of a trade union,
e. their physical or mental health or condition,
f. their sexual life,
g. the commission or alleged commission by them of any offence, or
h. any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Controller

A person (or organisation) who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

Processing

Covers almost anything which is done with or to the data, including:

- obtaining data
- recording or entering data onto the files
- holding data, or keeping it on file without doing anything to it or with it
- organising, altering or adapting data in any way
- retrieving, consulting or otherwise using the data
- disclosing data either by giving it out, by sending it on email, or simply by making it available
- combining data with other information
- erasing or destroying data

Useful resources

- Guidance and advice is available from Legal Services (https://intranet.birmingham.ac.uk/legal-services/What-we-do/Contact-us.aspx - login required).

- The Legal Services intranet (https://intranet.birmingham.ac.uk/legal-services/What-we-do/Data-Protection/DPA-Resources.aspx - login required) contains:

    - Data Protection Key Points and Reference Guide
    - Data Protection Toolkits
    - Breach/incident reporting guidance and reporting form
    - Privacy impact assessment guidance and template
    - Information for NHS Digital researchers
    - Link to the Canvas Data Protection Training.

- The Information Commissioner's Officer's website contains guidance on data protectionhttps://ico.org.uk/for-organisations/guide-to-data-protection/ .