BIRMINGHAM CITY UNIVERSITY

Data Protection Policy

Version 2.0

Contents

1. Document Profile and Control

Purpose of this Document: To provide the University's policy on the processing of personal data.

Sponsor Department: Legal Services and Compliance

Author: Head of Legal and Compliance

Reviewer / Review date: Information Governance Board (IGB).

Document Status: APPROVED

Amendment History			
Date	Version*	Author/Contributor	Amendment Details
04/10/16	0.1	Information Governance Manager	First Draft
05/10/16	0.2	General Counsel	Second Draft
11/07/17	1.0	General Counsel	Draft Approved
23/10/18	2.0	Senior Associate	Draft update for GDPR 2 DPA 2018

**Version control note: All documents in development are indicated by minor versions i.e 0.1;0.2 etc. The first version of a document to be approved for release is given a major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.*

For Approval By:	Date Approved	Version
Information Governance Board	11/07/17	1.0
University Executive Group	22/01/19	2.0

Published on	Date	By	Dept
i-City	19/09/17	General Counsel	Information Management

2. Introduction

The aim of the policy is to provide a framework for Birmingham City University ('BCU' or 'the University') to meet its obligations under Data Protection Laws.

The processing of personal data underpins almost everything the University does. For example, without it, students applications could not be processed, they could not be enrolled or taught; employees could not be recruited; research involving living individuals could not be undertaken; and events could not be organised for prospective students, alumni or visitors.

BCU is responsible for processing people's personal information and if this is not handled properly, the University could put individuals at risk.

There are also legal, financial and reputational risks for the University if personal data is not handled correctly. For example:

- Reputational damage from a breach may affect public confidence in our ability to handle personal information and impact on student engagement and student or employee recruitment;

- The Information Commissioners Office (ICO), which enforces the Data Protection Laws, has the power to fine organisations up to 4% of global annual turnover or €20 million for serious breaches;

- If BCU is not able to demonstrate that the University has robust systems and processes in place to ensure the proper use of personal data BCU could lose the ability to carry out research projects requiring access to personal data.

It is therefore essential that all employees, contractors or companies and other third parties holding, storing or using information for or on behalf of the BCU understand and comply with the obligations under the Data Protection Laws.

3. Scope

This policy covers all personal data that is processed by BCU. This policy is applicable to all employees, contractors or companies and other third parties holding, storing or using information for or on behalf of the BCU**.**

4. Principles

The processing of any personal data by BCU must comply with the Data Protection Laws and, in particular, the six data privacy principles. Additional guidance on these is available from the Information Management Team. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner;

- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;

- adequate, relevant and limited to what is necessary;

- accurate and, where necessary, up-to-date;
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the accountability principle requires BCU to be able to evidence compliance with these principles.

5. Commitment

The University handles large amounts of personal data and takes its responsibilities under Data Protection Laws seriously. It recognises that the mishandling of an individual's personal data may cause them distress or put them at risk of identity fraud. As a result, BCU is committed to:

- complying fully with the Data Protection Laws;
- where practicable, adhering to good practice, as issued by the ICO, the Office for Students or other appropriate bodies; and
- handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.

The University seeks to achieve the above aims by:

- ensuring that employees, students and other individuals who process data for University purposes are made aware of their individual responsibilities under the Data Protection Laws and how these apply to their areas of work. For example, employment contracts include a clause drawing the attention of the employee to the Data Protection Laws and the University's data protection policy;
- providing suitable training, guidance and advice. The University's online training on data protection and information security is available to all members of the University and is a mandatory requirement. The online modules are supplemented by bespoke on-site training, where appropriate, along with regular talks and presentations at University conferences and departmental meetings;
- incorporating data privacy requirements into administrative procedures where these involve the processing of personal data, particularly in relation to major information systems (the concept of 'privacy by design') and undertaking Data Privacy Impact Assessments when required;
- maintaining a University-wide register ('the Information Asset Register') exercise to capture the full range of processing that is carried out, the lawful basis of processing, the data security in place and any data risks;
- as far as is practicable, ensuring that all individuals whose personal data is processed by BCU are aware of the way in which that information will be held, used and disclosed by the University;
- including a 'fair processing' statement in collection forms requiring personal information giving details of who, why and for how long the information will be used;

- maintaining the central Privacy Notice on the BCU website at: https://www.bcu.ac.uk/privacy which covers how the University will use personal information;

- Implementing and maintain appropriate organizational and technical measures to protect personal data. In particular,

    - unauthorised staff and other individuals are prevented from gaining access to personal information;
    - appropriate physical security is in place and BCU buildings have reception areas or controlled access;
    - computer systems are installed with user-profile type password controls to ensure data is only accessed by authorised users;
    - where necessary, audit and access trails are monitored to establish that each user is fully authorised;
    - all portable media used for personal information is protected by encryption;
    - remote access to University systems is controlled using Multi Factor Authentication; and
    - manual filing systems are held in secure locations and are accessed on a need-to-know basis.

  Additional details are included in the University's Information Security Policy;

- maintaining retention and destruction procedures to ensure information is only retained for as long as is necessary and then deleted and securely destroyed;

- operating a centrally coordinated procedure (in order to ensure consistency) for the processing of subject access and other data rights based requests made by individuals; and

- investigating promptly any suspected breach of the Data Protection Laws; reporting it, where necessary, to the ICO; and seeking to learn any lessons from the incident in order to reduce the risk of reoccurrence.

- Implementing systems to only share information with other parties or third parties, where it is legal to do so, if this enhances the University's ability to improve student services, experience, research, development opportunities or employee related matters. Any information sharing arrangements concerning personal information (student, employee or other) will be based upon formal protocols and when relevant detailed in formal contracts, data sharing or data processing agreements.

- Maintaining and continuing its registration with the Information Commissioner's Office ('ICO'). The University's registration number is: Z7262717. The registration entry details are available on the ICO website at: https://ico.org.uk/ESDWebPages/Entry/Z7262717 .

6. Responsibilities

The University Board of Governors has overall responsibility for ensuring compliance with the Data Protection Laws.

The University Secretary and **Chief Finance Officer** has strategic responsibility for Information Governance including compliance with the Data Protection Laws throughout the University including registration requirements with the Information Commissioner's Officer.

The Head of Legal and Compliance and the **Data Protection Officer** are responsible for advising and providing guidance on matters concerning Data Protection and BCU's data protection obligations. They are also responsible for notification requirements to the Information Commissioner, such as reporting data breaches or consultations on Data Privacy Impact Assessments.

The Information Security Manager is responsible for information security in the University and provides relevant support for data protection related issues.

The Information Governance Board will monitor the implementation of this policy and internal compliance with the Data Protection Laws. It is also responsible for reviewing and approving policies and procedures to facilitate the University's compliance with the Data Protection Laws.

The Information Management Team is responsible for:

- establishing and maintaining policies and procedures at a central level to facilitate the University's compliance with the Data Protection Laws;
- establishing and maintaining guidance and training materials on data protection and specific compliance issues;
- supporting privacy by design and data privacy impact assessments;
- responding to requests for advice from faculties, schools and departments;
- supporting and providing advice on a University-wide register exercise to capture the full range of processing that is carried out ('the Information Asset Register');
- complying with subject access and other data rights requests made by individuals for copies of their personal data and or to exercise their other data rights;
- investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data); and
- keeping records of personal data breaches, notifying the ICO of any significant breaches and responding to any requests that it may make for further information.

  In fulfilling these responsibilities, the Information Management Team will be supported by the Information Governance Board, who may also involve, and draw on support from, representatives from, departments, faculties and schools as necessary.

Directors and **Senior Managers** are responsible for ensuring compliance with the Data Protection Laws and implementing the policy and all associated guidance within their individual faculties, schools or departments. In particular, they must ensure that:

- new and existing employees, visitors or third parties associated with the faculty, school or department who are likely to process personal data are aware of their responsibilities under Data Protection Laws. This includes drawing the attention of staff to the requirements of this policy, ensuring that employees who have responsibility for handling personal data are provided with adequate training and, where appropriate, ensuring that job descriptions for members of staff or agreements with relevant third parties reference data privacy responsibilities;
- adequate records of processing activities are kept (for example, by undertaking regular reviews and updates of the Information Asset Register);
- data protection requirements are embedded into systems and processes by adopting a 'privacy by design' approach and undertaking data privacy impact assessments where appropriate;
- privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;
- data sharing is conducted in accordance with University guidance;

- BCU's Multi Factor Authentication ('MFA') is enabled and used by all employees accessing BCU systems remotely;
- requests from the Information Management Team for information are complied with promptly and assistance and resource provided when required to respond to data right requests, breach investigations or complaints;
- data privacy risks are included in the Information Asset Register and/or local risk register and considered by senior management on a regular basis; and
- departmental policies and procedures are adopted where appropriate.

Individuals processing BCU data (including employees, temporary employees, students/volunteers, agents, contractors or suppliers): Anyone who processes personal data for BCU is individually responsible for complying with the Data Protection Laws, this policy and any other policy, guidance, procedures, and/or training introduced by the University to comply with the Data Protection Laws. In summary, they must ensure that they:

- only use personal data in ways people would expect and for the purposes for which it was collected;
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- keep personal data up-to-date;
- keep personal data secure, in accordance with the University's Information Security Policy;
- do not disclose personal data to unauthorised persons, whether inside or outside the University;
- complete relevant training as required;
- report promptly any suspected breaches of Data Protection Laws, in accordance with section 7 below;
- seek advice from the Information Management Team where they are unsure how to comply with Data Protection Laws or Data Protection policies; and
- promptly respond to any requests from the Information Management Team in connection with any data rights requests, breach investigations or complaints (and forward any such requests or complaints that are received directly to the Information Management Team promptly).

7. Breaches

The University will investigate incidents involving a possible breach of the Data Protection Laws including any near misses in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future. Depending on the nature and severity of the incident, it may also be necessary to notify the individuals affected and/or the ICO. A breach will occur where, for example, personal data is disclosed or made available to unauthorised persons or personal data is used in a way that the individual does not expect.

All data breaches must be reported in accordance with the the University's data breach reporting procedure. Advice and guidance on immediate action can also be obtained from the Information Management Team who can be contacted on 0121 202 2900.

Incidents involving failures of IT systems or processes should also be reported immediately to the BCU IT Helpdesk.

8. Data Rights

Under Data Protection Laws individuals have the following rights:

- to obtain access to, and copies of, the personal data that BCU holds about them;
- to request that BCU ceases processing personal data;
- to require BCU not to send marketing communications;
- to request corrections to the personal data BCU holds if it is incorrect;
- to request BCU to erase personal data;
- to request BCU to restrict data processing activities;
- where processing is based on consent, an Individual may withdraw that consent, without affecting the lawfulness of the processing based on consent before its withdrawal;
- to receive a copy of the personal data BCU holds about the individual, in a reasonable format for the purpose of transmitting that personal data to another data controller;
- to object, on grounds relating to an individual's particular situation, to any of BCU's particular processing activities where it has a disproportionate impact on the individual's rights.

The above rights are not absolute and BCU may be entitled to refuse requests where exceptions apply.

With the exception of data access/subject access requests (see below) BCU will reply to a data right request as quickly as possible and in all cases will issue a decision notice or provide an update within 20 working days. BCU will issue a decision notice in relation to all requests to exercise a data right. The notice will explain if the request has been granted, granted in part or refused. Where any request is refused or only granted in part reasons will be provided to explain why. All notices will also include any appeal rights.

In relation to data access/subject access requests BCU will reply to subject access requests as quickly as possible and in all cases within one calendar month allowed by the Data Protection Laws. The University will endeavor to fulfil all legitimate and reasonable requests. In some cases, especially with requests that are not clear, further information may be required from the requester which may delay the start of the time limit.

The Information Management Team is responsible for processing all data right requests and maintaining adequate records of the requests and outcomes.

If an individual wishes to exercise any data right, they can contact the University's Data Protection Officer using the following contact details:

By Email to: informationmanagement@bcu.ac.uk

By Telephone on: +44 (0)121 202 2900

By Post to: Data Protection Officer
Information Management Team
Birmingham City University
University House
15 Bartholomew Row
Birmingham
B5 5JU

9. Data Protection Complaints

Complaints regarding data protection should be sent to the Data Protection Officer at informationmanagement@bcu.ac.uk or by writing to: The Data Protection Officer, Birmingham City University, 15 Bartholomew Row, Birmingham, B5 5JU.

Any complaint must be written, dated and must include details of the complainant as well as a detailed account of the nature of the problem. BCU will aim to provide a substantive response within twenty working days and in every case the person will receive an acknowledgement within three working days of the complaint being received.

The BCU complaints procedures outlines how a complaint regarding any other matter can be made to the University, and what you can expect from BCU in processing that complaint.

10. Further Information

Questions about this policy and data privacy matters in general should be directed to the Information Management Team at: informationmanagement@bcu.ac.uk.

Questions about information security should be directed to the Information Security Team at: ITSecurityTeam@bcu.ac.uk.

11. Enforcement

The University regards any breach of the Data Protection Laws, this policy or any other policy and/or training introduced by the University from time to time to comply with the Data Protection Laws as a serious matter, which may result in disciplinary action, under the University's disciplinary procedure. Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of the University to disclose personal information unlawfully).

12. Related documents

Definitions used in this policy are included at Appendix 1.

This policy should be read in conjunction with related policies, procedure and guidance, which provides further detail and advice on practical application, including the:

- Information Security Policy
- Data Breach Reporting Procedure

13. Implementation Plan

Intended Audience	All BCU employees.
Dissemination	Available to all employees via iCity and to the public via the BCU publication scheme.
Communications	To be announced via email to senior management, Data Protection Co-ordinators with hyperlink for cascade to team members and promoted by the Information Governance Board and Information Management Team.
Training	New staff will be provided with training at their Corporate Induction and as part of their local induction. All staff are required to complete an online training module regarding *Data Protection.* Appropriate training refresher courses for Information Governance and Data Protection training will be designed and implemented. Faculties and departments can also request bespoke training from the Information Management Team. Data Protection Co-ordinators will received more detailed training.
Monitoring	Results on the effectiveness will be included in reports to the IGB and any changes or amendments will be documented in a new version of the policy.

Appendix 1 – Definitions

Personal Data	personal data is data about a living individual. That living individual must be identifiable, either directly or indirectly, through an identifier such as name, student number, email address, or online identifiers such as an IP address. For further guidance and examples, see **Appendix 2**.
Processing data	means obtaining, recording, holding, sharing, and retaining and deleting of personal data and takes the same meaning as defined within data protection law.
GDPR	means the General Data Protection Regulation 2016/679.
DPA	means the Data Protection Act 2018.
Data Protection Laws	means the GDPR 2016/679, the DPA, the Privacy of Electronic Communications Regulations 2003 any other applicable data protection laws that apply to processing of Personal Data by the University and its subsidiaries.
DPIA	means Data Protection Impact Assessments required under Article 35 of the GDPR.
Data Rights	means the right to be informed; the right to access; the right to object; the right to rectification; the right to restriction; the rights to erasure; the right to data portability and rights in relation to automated decision making and profiling.
DPO	means the Data Protection Officer

Appendix 2 – Personal Data

The following are (non-exhaustive) examples of the types of data that can constitute 'Personal Data':

- Name;
- Data of Birth/Age;
- Postal Address(es) (to include postcodes);
- Contact telephone number(s);
- Email address(es);
- Unique Identifiers (to include: Student ID numbers, Staff ID numbers, Passport numbers, NHS numbers, National Insurance numbers, unique research participant ID numbers, Unique applicant ID numbers, vehicle reg, driving licence numbers);
- Images of individuals, including CCTV, photos;
- Location Data (to include any GPS tracking data);
- Online Identifiers (to include IP address data);
- Economic/financial data (relating to an identifiable individual);
- Educational records including but not limited to records held by the University and other education providers;
- Counselling records;
- Pastoral records, including Extenuating Circumstances Forms;
- Disciplinary records;
- Training records;
- Employment records to include CV's, references;
- Nationality/Domicile;
- Ethnicity;
- Mental Health (status, medical records conditions, to include disability);
- Physical Health (status, medical records conditions, to include disability);
- Dietary requirements;
- Sexual Orientation/Sexual life;
- Genetic Data (to include DNA data);
- Biometric data (such as facial image or fingerprint data);
- Political opinions;
- Trade Union membership;
- Religious or philosophical beliefs; and
- Criminal Convictions and offences (to include alleged offences and convictions).