BIRMINGHAM CITY UNIVERSITY

Data Protection Policy

Version 1.0

Contents

Document Profile and Control

Purpose of this Document: To provide a framework to manage Data Protection Act, 1998 requirements and lay a foundation for the implementation of further requirements to ensure compliance with the General Data Protection Regulation ('GDPR') by May 2018.

Sponsor Department: Information Management Team

Author: General Counsel

Reviewer / Review date: Information Governance Board (IGB). To be reviewed: April 2018

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

***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

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

Introduction

The Data Protection Act 1998, (the DPA) extends rights of individuals and requires data controllers (people or organisations that hold and process the details of living individuals) to comply with the Eight Principles (rules governing the use of personal data – see Appendix 1) and to bear in mind the rights and freedoms of those individuals when processing their details.

This document explains how Birmingham City University ('BCU' or 'the University') will meet the legal requirements of the DPA. Measures within the policy will also lay a foundation for the implementation of further requirements to ensure compliance with the General Data Protection Regulation ('GDPR') by May 2018

Scope

This policy covers all personal information 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.

Objectives

1. To provide a framework to manage the Data Protection Act 1998 requirements;

2. To provide guidance to employees and third parties that explains the requirements of the Act and their responsibilities with regard to managing an individual's personal information.

Responsibilities

The University **Board of Governors** has overall responsibility for ensuring that compliance with the Data Protection Act 1998 is managed responsibly within the University.

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

The **Data Protection Officer** is responsible for the management of corporate processes concerning Data Protection including notification to the Information Commissioner.

The **IT 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.

The **Directors** and **Senior Managers** are responsible for ensuring that the policy is implemented in their directorates and individual departments.

Statement of Intent

BCU intends to fulfil all its obligations under the Act. The University will ensure that the Information Commissioner is notified of all relevant processing and will conduct an annual

review and update of the Notification Scheme to ensure that it remains up to date. It is the aim of the University that all appropriate staff are properly trained, fully informed of their obligations under the Act and are aware of their personal responsibilities.

BCU will only share information with other parties or third parties, where it is legal to do so, if this enhances its ability to improve student services, experience and research and development opportunities. Any information sharing arrangements concerning personal information (student, employee or other) will be based upon formal protocols and will be in accordance with the DPA's eight Data Protection principles (see Appendix 1).

BCU will secure and maintain in accordance with the Act such data as is necessary to assist in the protection of the health and safety of its employees and students while continuing to comply with obligations under the DPA.

Individuals whose information is held and processed by BCU can be assured that it will treat their personal data with all due care.

Where the University is not the data controller but rather the data processor it will abide by any written agreement between it and the data controller on data protection policy. This means where we process data collected by others. For example, in connection with partnership working or under certain research and development contracts and agreements.

This policy document applies only to information covered by the DPA and will be updated as necessary according to the laws of England and in accordance with the GDPR.

Separate codes of practice exist or are being developed within BCU in respect of the following types of processing:-

- Security - including: CCTV, telephone, internet and e-mail usage, disposal of confidential waste, manual records and the security of buildings.

- Policy for Access to Students/Employee Records - including student/employee access to their own records and the disclosure of student and or employee Information.

- Records Management Retention and Disposal Policy and Procedure on the length of time records must be held.

- Data sharing – including procedures for standard contractual terms and or data sharing agreements

- Processing and notifications requirements – including procedures for appropriate fair processing notices (privacy notices), recording of the information internally and reporting and updating of processing registrations with the Information Commissioner's Office

Fair Obtaining/Processing

The University will, as far as is practicable, ensure that all individuals whose details it holds are aware of the way in which that information will be held, used and disclosed.

Individuals will, where possible and practicable, be informed of the likely recipients of the information – whether the recipients are internal or external to the University.

Processing within the University will be both fair and lawful and individuals will not be misled as to the uses to which BCU will put the information given. If a person feels they have been deceived or misled as to the reason for which their information was collected, they should report this to the information management team detailed at the end of this policy document.

Collection forms requiring personal information will contain a 'fair processing' statement giving details of who, why and for how long the information will be used. Where information is collected in person or by telephone, the employee asking for the details will tell the individual how those details will be used, who will use them and for how long the information will be kept. People are free to ask the person collecting the information why they want the details and what they will be used for. There is a Fair Processing (Privacy) Notice on the BCU website which covers how the University will use personal information.

Where the University is using an exemption under the DPA to obtain personal information that, in all of the circumstances, makes a fair obtaining statement impractical then no such statement will be made. Examples of this would be where a serious medical or criminal incident occurs on University premises and the taker needs to focus on collecting data that is time critical in order to protect the vital interests of an individual.

Any personal information processed falls into one of two categories under the DPA. These two types are personal data and sensitive personal data. Processing of these types of data require conformance with one set of conditions with regard to personal data and two sets of conditions when sensitive data is processed. A summary of the processing conditions is at Appendix 2.

If a person's details are going to be used for automated processing (where a computer decides something based on a score or other information) the person will be entitled to be told about how the scoring system works and whether the decision can be challenged.

Data Uses and Processes

The University will not use or process personal information in any way that contravenes its notified purposes or in any way that would constitute a breach of Data Protection law.

If a person's details are to be processed for a new purpose that does not appear on the University's notification scheme (e.g. some new processing not previously notified to the ICO) the individual will be given the information and or consent obtained that would be necessary to make the processing fair and lawful. BCU will also undertake to review its notification documents and make a formal updated notification to the Information Commissioner as soon as possible when appropriate.

A copy of the appropriate notification document is available from the Information Management Team. The BCU Notification Scheme can also be viewed on the Information Commissioner's web page: https://ico.org.uk/ESDWebPages/Entry/Z7262717

All staff using personal data within the University will be told the limits of their authority to use and disclose such information through their managers, the induction process and training.

All new purposes are to be documented and notified to the Information Management Team to consider making formal update notifications to the Information Commissioner as soon as possible when appropriate.

Data Quality and Integrity

BCU will not collect data from individuals where that information is excessive or irrelevant in relation to the notified purpose(s). Details collected will be adequate for the purpose and no more. Information collected which becomes (over time or by virtue of changed purposes) irrelevant or excessive will be deleted and destroyed in accordance with the University retention and destruction policy.

All of the University faculties/departments will manage data collection and updating of records such that accuracy, relevance, consistency with purpose and quality are assured.

Information will only be retained for as long as is necessary for the notified purposes(s), after which the details will normally be deleted and destroyed in accordance with the University retention and destruction policy. Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records it will always be done within the requirements of the DPA. In some cases records will be sanitised or appropriately redacted so that individuals cannot be identified.

The University will ensure, as far as is practicable, that the information held is accurate and up to date. It is the intention of BCU to check wherever possible the details given. Information received from third parties (i.e. neither the individual concerned nor BCU records) will indicate the source, where practicable.

Where a person informs BCU of a change of their own circumstances, such as home address or non-contentious data, their record(s) will be updated as soon as possible. Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, a comment will be placed on the disputed record indicating the nature of the problem. If the system does not allow the individual record to be marked in this way, departments will ensure that a manual record is made of the request and that it is processed within a reasonable time-scale.

Every effort will be made to reach an amicable agreement on any disputed data. Where this is not possible BCU will implement its complaints procedure.

An internal investigation will be implemented if there is any alleged improper misuse of personal data by staff and appropriate action will be taken.

If any employee suspects any weaknesses in the security of any information processing systems or suspects staff misuse with regard to data protection they should contact the IT Security Manager or the Data Protection Officer as appropriate.

Technical and Organisational Security

The University has implemented appropriate security measures as required under the DPA. These are set out in full in the University's Information Security Policy. In particular, unauthorised staff and other individuals are prevented from gaining access to personal information. Appropriate physical security is in place and all 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, and where necessary, audit and access trails are monitored to establish that each user is fully authorised. In addition, all portable media used for personal

information is to only be used if protected by appropriate encryption. Manual filing systems are held in secure locations and are accessed on a need-to-know basis only.

The Information Security Work Group (ISWG) will regularly review Security arrangements and all reported breaches of security will be investigated. Where necessary, further or alternative measures will be introduced.

Where details need to be passed outside the University it will in general be done with the person's consent except where this is not possible or where it is required by law, i.e. the use of exemptions specified under the Act (such as crime prevention/detection, prevention of injuries etc.) or where it is in the person's vital interests. Any unauthorised disclosure will be dealt with under the University's disciplinary procedures.

Redundant personal data will be destroyed as confidential waste in line with the University's retention and destruction policy. In general, paper waste is outside certified shredding contractors and magnetic media (disks, tapes, etc.) are either electronically wiped or physically destroyed beyond recovery.

Subject Access/Subject Information Requests

The DPA gives individuals the right to see information held about them and places a duty on the University to make that information available. Thus any person whose personal details are held/processed by BCU has a right to receive a copy of his or her own information. There are a few exceptions to this rule (examples being data held for child protection, crime detection/prevention purposes or where the information is likely to cause serious harm to the physical and/or mental health of an individual) but most individuals will be able to have a copy of the data held about them.

Where any information relates to an identifiable third party, other than the data subject, consent will be gained from that third party, unless a legal exemption applies before any information relating to them can be released.

BCU has the right to make a charge for such requests for computer based data and data held on paper or other media. An appropriate charge will be levied for this in line with applicable charging schemes. Any codes or abbreviations used in the record will be explained.

Subject access requests from students, the public or solicitors acting on behalf of the students or the public will be handled by the Information Management Team. Requests from employees and former-employees will be handled by Human Resources who may transfer the request to be handled by the General Counsel.

BCU will reply to subject access requests as quickly as possible and in all cases within the 40 days allowed by the DPA. Repeat requests will be fulfilled unless the period between is deemed unreasonable, such as a second request received so soon after the first that it would be unlikely for the details to have changed. The University will endeavour 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 40 day maximum time limit.

Procedures for the processing and handling of subject access requests are to be developed.

Further Information and Enquiries

The Information Management Team is the first point of contact for the issues mentioned in this policy document and will handle all internal and external enquiries regarding data protection and subject access requests. Where possible, requests for detailed information should be in writing.

Requests regarding any data protection matters and or any concerns over how data is being processed should be sent to the Data Protection Officers at: informationmanagement@bcu.ac.uk.

Enforcement

Any employee deliberately acting outside of their authority or otherwise in breach of this policy or other policies or procedures supporting it, may be subject to the University's disciplinary procedure

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 reported to UEG.
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 mandatory 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

The Data Protection Act, 1998: the eight principles

In order to process personal information in line with the Act, the following eight principles regarding privacy and disclosure must be satisfied.

First Principle

'Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- *at least one of the conditions in Schedule 2 is met; and*
- *in the case of **sensitive personal data**, at least one of the conditions in Schedule 3 is also met.'*

Second Principle

'*Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'*.

Third Principle

'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'.

Fourth Principle

'*Personal data shall be accurate and, where necessary, kept up to date'*.

Fifth Principle

'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'.

Sixth Principle

'Personal data shall be processed in accordance with the rights of data subjects under this Act'.

Seventh Principle

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'.

Eighth Principle

'Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data'.

Appendix 2

Summary of Relevant Conditions for Processing Data

Schedule 2 Conditions

In all cases data controllers must satisfy at least one of the conditions in Schedule 2 of the Act, in summary this includes:

1. The data subject has given consent
2. The processing is necessary:
    a. for the performance of a contract to which the data subject is a party; or
    b. taking steps requested by the data subject with a view to entering a contract
3. The processing is necessary for compliance with a legal obligation (other than imposed by a contract)
4. The processing is necessary to protect the vital interest of the data subject
5. The processing is necessary for the administration of justice, functions of either House of Parliament, any exercise of function conferred on any person by or under any enactment, any function of the crown or government department or the any function of a public nature exercised in the public interest.
6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

When sensitive data is processed, at least one Schedule 3 processing conditions must be met.

'Sensitive data' is defined in the Act and includes data that relates to any of the following:

(a) racial or ethnic origin
(b) political opinions
(c) religious beliefs or other beliefs of a similar nature
(d) whether an individual is a member of a trade union
(e) physical or mental health or condition,
(f) sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of any court in such proceedings

Schedule 3 Conditions

The Schedule 3 conditions include:

1. The data subject has given explicit consent.

2. To exercise or perform any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

3. To protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The information has been made public as a result of steps deliberately taken by the data subject.

5. For legal proceedings (including prospective legal proceedings), when necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

6. For medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

   "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

7. Information as to racial or ethnic origin, necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and is carried out with appropriate safeguards for the rights and freedoms of data subjects.

8. When processed in circumstances specified in an applicable order made by the Secretary of State.