BIRMINGHAM CITY UNIVERSITY

Data Protection Policy

and

Appropriate Policy Document

Version 3.3

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

Author: Data Protection Officer

Approver / Approval date: IGB 11.09.2024

Document Status: Approved

Table showing 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
17/12/20	2.1	Data Protection Officer	Scope and student responsibilities section 6
19/04/22	2.2	Data Protection Officer	Review to reflect UK GDPR, inclusion of Sharing Personal Data and Direct Marketing sections.
12/09/22	2.3	Data Protection Officer	Updates following IGB actions and addition of Appendix 4.
09/12/22	2.4	Data Protection Officer	Updates following IGB actions and addition of App 4
16/01/23	3.0	Data Protection Officer	Finalised version following UEG review.
28/06/2023 and again on 20/04/2024	3.1	Data Protection Officer	Updates include information about sharing data with a nominated person and to include the Appropriate Policy Document
03/01/2024	3.2	Data Protection Officer	Update to match the example data breach form included in this document with most up-to-date data breach form.

11/09/2024	3.3	Information Governance Board	Updates in the Appropriate Policy Document to include reference to the Students with Criminal Convictions Policy and Procedure, and to clarify and add wording related to conditions of processing special category data and criminal offence data.

**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
Information Governance Board	28/04/21	2.1
University Executive Group	10/01/23	3.0
Information Governance Board	28/06/23	3.1
Information Governance Board	20/03/24	3.2
Information Governance Board	11/09/24	3.3

Published on	**Version**	**Date**	**By**	**Dept**
i-City	1.0	19/09/17	General Counsel	Information Management
i-City & BCU Website	2.0	22/01/19	Data Protection Officer	Information Management
i-City & BCU Website	2.1	05/05/21	Data Protection Officer	Information Management
i-City & BCU Website	3.0	16/01/23	Data Protection Officer	Information Management
i-City & BCU Website	3.1	10/07/23	Data Protection Officer	Information Management
BCU Website. i-City link now links directly to	3.1	03/01/23	Data Protection Officer	Information Management

BCU website.				
BCU Website Policy and Procedures page	3.2	20/03/24	Data Protection Officer	Information Management
BCU Website Policy and Procedures page	3.3	14/10/24	Data Protection Officer	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, student's 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. Details on the scope of information held by the University which is likely to encompass 'personal data' can be found in Appendix 2.

BCU is responsible for processing people's personal information and if this is not handled in accordance with the Data Protection Laws, 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 Data 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 £17.5 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 funded 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, 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 including its subsidiaries and relevant partnerships. This policy is applicable to all employees, contractors or companies and other third parties holding, storing or using information for, or on behalf of, BCU.

Student's responsibilities when processing personal data as part of their studies at Birmingham City University ('BCU') are set out in section 6.

4. Principles

The processing of any personal data by BCU must comply with the Data Protection Laws and, in particular, the data protection 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, put them at risk of identity fraud or some other form of harm. 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 University employees and is a mandatory requirement. The online modules are supplemented by bespoke training, where appropriate, along with regular awareness activity and interactions with faculties and departments;
- 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 DPIAs when required;
- maintaining a University-wide register ('the Information Asset Register' and 'Record of Processing Activity) to capture the full range of processing that is carried out, the lawful basis of processing, the data security in place and any associated 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 'privacy notice' statement in collection forms requiring personal information,

giving details of BCU, why we are collecting the personal data and for how long the information will be used;

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

- Implementing and maintaining 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;
    - when individuals are working away from the office, they follow best practice approaches to securing personal data, as specified in Appendix 4;
    - computer systems are installed with access controls, such as passwords and multi-factor authentication 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;

- 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, and those of any commercial entities under BCU control, with ICO. The University's registration number is: Z7262717. The registration entry details are available on the ICO's Register of Data Protection Fee Payers.

6. Responsibilities

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

The University Executive Group has responsibility for ensuring compliance with the Data Protection Laws across BCU and assuring the Board of Governance of appropriate compliance activities taking place. This responsibility is supported by the roles and groups noted below.

The Head of Legal Services 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 DPIAs; together with maintaining the University's registration with the Information Commissioner's Office.

The Associate Director of IT Security and Compliance is responsible for information security within the University and provides relevant support for data protection issues involving the security of electronic records and due diligence considerations alongside other IT colleagues.

The Information Governance Board provides the strategic direction for Information Governance and 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 DPIAs;
- responding to requests for advice from faculties, schools and departments;
- supporting and providing advice on a University-wide register exercises to capture the full range of processing that is carried out (through the Information Asset Register and Record of Processing Activity);
- support the due diligence of Data Processors and advise on the need for formal contracts, data sharing or data processing agreements;
- complying with subject access and other data rights requests made by individuals for copies of their personal data and or to exercise their other personal data rights;
- investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data) received from data subject or the ICO; 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.

Legal Services will support (or assist to procure) legal advice and guidance on data protection matters, where required. They will also support the review of formal agreements with third parties involving the exchange of personal data alongside the Information Management Team.

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 protection responsibilities;
- adequate records of processing activities are kept (including 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 DPIAs 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 rights requests, Breach investigations or complaints;
- data privacy risks are included in the Information Asset Register and/or local risk register and reviewed and updated by senior management on a regular basis; and
- departmental policies and procedures are adopted to further protect personal data 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 support compliance with the Data Protection Laws. In summary, they must ensure that they:

- only use personal data in ways individuals 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, including your own personal data held in BCU systems such as the ERP;
- keep personal data secure, in accordance with the University's Information Security Policy;
- use BCU core systems to access and record activity related to individuals in accordance with local processes or procedures;
- 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).

Students processing personal data as part of their studies at BCU must ensure that they:

- inform individuals on how their data will be used, if collected directly;
- only use personal data in ways individuals 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; and,
- seek advice from their lecturer or personal tutor where they are unsure how to comply with Data Protection Laws or Data Protection policies.

7. Sharing Personal Data

As defined in the Data Protection Laws, BCU acts at the Data Controller for the majority of the personal data it processes, as the University decides what personal data to collect and how it will be used. We will also engage suitable organisations to act as Data Processors where they will process personal data on the University's behalf; where this occurs, we must undertake suitable due diligence before contracting with them.

In some situations, such as where BCU is completing a research project on behalf of a third party using their customer or client base contact information, BCU will act as a Data Processor for a third party. Where this occurs BCU should be subject to a specific data processing agreement identifying how BCU will process that data on behalf of the third party.

The University may also enter into Information Sharing Agreements with third party organisations where there is a legal requirement or relevant lawful basis to share personal data with them. This may be on a Data Controller to Data Controller basis and is likely to require a formal data sharing agreement.

Where any data is be shared outside of the university advice must be sought from the Information Management Team to determine if the process needs to be annotated within a formal contract, data sharing or data processing agreement, The Information Management Team will support those considerations and any relevant due diligence with assistance from IT Security and Legal Services where relevant.

Sharing of personal information with a student's nominated person

Birmingham City University has a requirement to treat all students as adults and does not act in loco parentis ("in the place of a parent") in relation to students, regardless of their age. In accordance with data protection laws there are limited situations where the University shares personal information about students or discusses their circumstances. Outside of an emergency, the University will only share such information with a student's nominated person (for example a partner, relative, friend or associate) with explicit written consent from the student, where the University is satisfied that this consent has been provided voluntarily by the student and that they have not been coerced into providing this consent. The student needs to provide written consent* via their Birmingham City University email account, or in person, as decided by the relevant University service or area. This consent allows the University to share personal data

about the student with the student's nominated person but does not permit that person to act on behalf of the student. The correspondence should always include the student's BCU email address to ensure that the student remains fully informed.

Although those under 18 years of age are regarded as children under the law, they still have the right, under data protection laws, for information about them not to be disclosed without their consent. This means that, whether or not someone is over 18 years of age, the University is not able to give information to relatives regarding a person's status at the University (e.g. whether or not they are an applicant, student or alumni, member of staff etc.), a student's attendance, progress, results or any other personal circumstance unless that person (the applicant, student, alumni, member of staff etc.) has given their specific consent or in the circumstances outlined above. However, if a student fails to pay any sums agreed on contract, then it will be necessary to disclose this to the student's guarantor, whether or not that person is the student's nominated person.

If someone submits a Data Subject Access Request on behalf of someone else, the University needs to satisfy itself that the person making the request has the data subject's permission to act on their behalf and that the data subject wants the DSAR to happen.

* By default, references to consent mean written consent, but may be interpreted in an appropriate way, agreed by all parties, to take account of disabilities. Where a student is unable to give consent, for example, due to an incapacity, the Data Protection Officer, a member of the University Executive Group or senior member of Student Support staff and other staff where appropriate, will consider the situation on a case-by-case basis.

An emergency situation refers to a situation where vital interests would be an applicable lawful basis for sharing personal data, rather than consent.

8. Breaches

The University will investigate any incidents involving a possible Breach of the Data Protection Laws including any near misses 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 manner which is contrary to the Data Protection Laws and this policy.

All Data Breaches must be reported in accordance with the University's data breach reporting procedure, see Appendix 3 for Data Breach Report Form. Advice and guidance on immediate action can also be obtained from the Information Management Team.

Incidents involving failures of IT systems or processes should be reported immediately to the BCU IT Helpdesk, if the incident involves personal data you must also report this to the Information Management Team.

9. Data Rights

Under Data Protection Laws individuals have the following rights:

- to be told how we will process their personal data;
- to obtain access to, and copies of, the personal data that BCU holds about them;

- to request that BCU ceases the processing of their personal data;
- to require BCU not to send marketing communications;
- to request corrections to the personal data BCU holds, if it is inaccurate;
- to request BCU to erase personal data;
- to request BCU to restrict data processing activities;
- to withdraw their consent to the processing of their personal data where consent is the legal basis is used by BCU, this does not affect the lawfulness of the processing based on consent before its withdrawal;
- of data portability, which provides for a copy of their data in a format to allow reuse for their own purposes with another organisation;
- to object to the processing of their data in certain circumstances;
- rights in relation to automated decision making and profiling; and,
- to complaint to the ICO about BCU's handling of their data.

The above rights are not absolute and BCU may be entitled to refuse requests where exceptions apply or the specific right is not applicable to the type of processing undertaken.

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 response within one calendar month. The response will explain if the request has been granted, granted in part or refused. Where any request is refused or only granted in part an explanation of BCU's decision will be provided. All responses will also include relevant appeal rights to the DPO and/or ICO.

In relation to data access/subject access requests BCU will reply to subject access requests as quickly as possible and within the timescales allowed by Data Protection Laws, which is one calendar month unless a two-month extension is applied. 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 time limit. The Subject Access Request Procedure is available on the BCU Policies and Procedures webpage.

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 Post to: Data Protection Officer
Information Management Team
1st Floor, Joseph Priestly Building
6 Cardigan Street
Birmingham
B4 7RJ

Where appropriate as a reasonable adjustment under the Equality Act 2010, an individual can call 0121 202 4597 or submit a voice recording or video recording instead of a written communication.

If a rights request is received locally by a faculty, school or department this must be promptly sent to the Information Management Team using the details above.

10. Direct Marketing

In addition to BCU's obligations under the UK GDPR, it is also subject to more specific rules in relation to direct marketing by email, fax, SMS or telephone. The University must ensure that it has appropriate consent from individuals to send them direct marketing communications, and that when a data subject exercises their right to object to direct marketing it has honoured such requests promptly.

Prior to the release of any direct marketing campaign relevant teams must ensure that appropriate UK GDPR compliant consents are held for the relevant audience. Further advice and guidance on the management of consents can be provided by the Information Management Team.

11. Data Protection Complaints

Complaints received regarding data protection should be sent to the Data Protection Officer at informationmanagement@bcu.ac.uk or forwarded to the address noted above.

Any complaint must be written (unless adjusting for Equality Act 2010 reasonable adjustments), dated and must include details of the complainant as well as a detailed account of the nature of the problem. Where appropriate as a reasonable adjustment under the Equality Act 2010, an individual can call 0121 202 4597 or submit a voice recording or video recording instead of a written communication. BCU will aim to provide a substantive response as quickly as possible and within one calendar month. In every case the complainant should 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.

12. Further Information

Questions about this policy and data protection 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: itsecurityhelp@bcu.ac.uk.

13. Enforcement

The University regards any breach of the Data Protection Laws, this policy or any other related policy and/or training introduced by the University from time to time to comply with the Data Protection Laws, as a serious matter. Any such breach may result in disciplinary action, under the University's Disciplinary Policy, which in the most severe situation may lead to dismissal. 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 an individual to unlawfully disclose University-held personal information with malicious intent.

14. 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
- Subject Access Request Procedure

15. Implementation Plan

Intended Audience	All BCU employees.
Dissemination	Available to all employees via iCity and to the public via the BCU website Policies and Procedures | Birmingham City University (bcu.ac.uk)
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 receive 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.

16. Appendix 1 – Definitions

Data Breach (Breach)	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
Data Controller	Organisation which determines the purposes and means of processing of personal data.
Data Processor	A third party that processing personal data on behalf of a Data Controller.
Data Protection Laws	means the UK GDPR, 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.
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.
DPA	means the Data Protection Act 2018.
DPIA	means Data Protection Impact Assessments required under Article 35 of the UK GDPR.
DPO	means the Data Protection Officer.
UK GDPR	means the UK General Data Protection Regulation (as incorporated into UK law under the UK European Union (Withdrawal) Act 2018) as amended in accordance with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

17. 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) (including postcodes);
- Contact telephone number(s);
- Email address(es);
- Unique identifiers (including: student ID numbers, staff ID numbers, passport numbers, NHS numbers, National Insurance numbers, unique research participant ID numbers, unique applicant ID numbers, vehicle registration number, driving licence numbers);
- Images of individuals, including CCTV and photographs;
- Location data (including GPS tracking data);
- Online Identifiers (including 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, including CV's and references;
- Nationality/domicile;
- Ethnicity;
- Mental health (status, relevant medical records);
- Physical health (status, medical records of conditions, including disability);
- Dietary requirements;
- Sexual orientation/sexual life;
- Genetic data (including DNA data);
- Biometric data (such as facial image or fingerprint data used to identify an individual);
- Political opinions;
- Trade union membership;
- Religious or philosophical beliefs; and
- Criminal convictions and offences (including allegations of an offence).

18. Appendix 3 – Personal Data – Data Breach Report Form

This form can be downloaded from the Data Breach Reporting Procedure webpage.

Data Breach Report Form

Please complete as much as the form as possible and send it to informationmanagement@bcu.ac.uk The more information you provide the less we will need to follow up with you.

If you have logged the incident with IT Services, please cc informationmanagement@bcu.ac.uk on the correspondence with IT where possible.

Do not include any personal data involved in the incident.

If the breach was caused through the sending of an email, please try to recall that email straight away, before filling in this form. You can update the Information Management Team later whether the recall was successful.

N.B. 'Data subject' is the term used for a living human being who the personal data is about.

Information Management reference number:	*Information Management team will add this.*
Information asked for:	**Information provided:**
Name and email address of person reporting the breach / near miss:	
Name and email address of who identified the breach / near miss: (If different to the person reporting)	
Name and email address of who caused the breach / near miss (if known):	
If you have contacted IT Services about this incident, please provide service request number and key contact if possible.	
What are you reporting?	☐ Near miss (e.g. email successfully recalled before it was read, work laptop with security active (e.g. password protected on) found undamaged. ☐ Data breach ☐ Not sure
Which type(s) of data breach / near miss are you reporting?	☐ Confidentiality – i.e. personal data being accessible to / accessed by someone who should not have had access. ☐ Integrity – i.e. personal data being corrupted / altered when it should not have been, AND another accurate copy is not available. ☐ Availability – i.e. personal data which should be available not being available AND there is no feasible

	workaround (e.g. database has crashed / blocked by ransomware and there is no suitable available backup).
Has the person who caused the breach / near miss completed data protection and information security training in the last two years?	☐ Data Protection (GDPR) ☐ Information Security ☐ Not known ☐ N/A (for example, if caused by an external person)
Date and approximate time of incident:	
Date and time the incident was identified:	
What happened? i.e. what is the data breach / near miss and how did it happen?	
Number of data subjects (i.e. individuals whose personal data was part of the data breach / near miss):	
List personal data affected by the breach, making clear whose personal data: *e.g. Student first names and surnames, student ID, student BCU and personal email addresses, student assessment results, staff emails about a student's reasonable adjustments / disability.* *Staff first names and surnames, staff job titles, staff NI number, staff DOB. etc.*	
Please tick if any of the categories of personal data have been included in this data breach or near miss (this list is of personal data generally considered higher risk).	☐ biometric data (for ID purposes i.e. RFID chips in passports /fingerprints / retina scan data) ☐ genetic data (n.b. someone's gender is not genetic data) ☐ philosophical beliefs ☐ physical or mental health information ☐ political beliefs ☐ race, or ethnic origin ☐ religious beliefs ☐ sex life ☐ sexual orientation ☐ trade union membership information ☐ complaint / disciplinary / grievance information ☐ criminal convictions and offences or related security measures ☐ economic and financial data, e.g. credit card numbers, bank details ☐ passwords, passcodes, PIN numbers

	☐ usernames that are not BCU email addresses ☐ other information that you consider could cause distress or embarrassment to the data subject. Please give details:
What relationship does the data subject have with BCU?	The data subject(s) is / are: ☐ Associate role providing services to BCU (e.g. contractors, agency staff etc. See list on this iCity page. ☐ Applicant to study at BCU ☐ Current Student ☐ Employee – current ☐ Employee - former ☐ Job applicant ☐ Member of the public ☐ Research participant ☐ Someone from a different organisation (please specify): ☐ TNE partnership or UK partnership staff member (please specify): ☐ Other (please specify):
Do the data subject(s) know about the breach?	☐ Yes ☐ No ☐ Don't know ☐ Some of them – please give details:
If a breach of Confidentiality, how many people has the personal data has been inappropriately exposed to.	
If a breach of Confidentiality, who had access to / accessed the personal data who should not have had access? What relationship do they have to BCU, if any? E.g. are they an applicant, current / former student, staff member, external organisation, member of public?	
The rest of the questions are for all types of data breach.	
What, if any, protective measures were in place? *e.g., encryption/password protected, pin-coded device, back-ups.*	

Brief description of any action already taken to resolve the situation and reduce the risks. (For example, recall of email or contacting a recipient of a data breach to ask them to delete it, or lost data has been recovered).	
What further actions could be taken to resolve the situation or reduce the risks of this specific breach? (Ignore if it's a near miss)	
What is the current or likely negative impact on the data subject that their personal data is part of this data breach? (Ignore if it's a near miss)	
Please provide any comments/suggestions on how reoccurrence of the breach / near miss can be prevented in the future.	
Any additional information you think it would be helpful to include:	

Thank you very much for completing as much information as possible. Please send to informationmanagement@bcu.ac.uk

19. Appendix 4 – Remote Working – Data Protection Requirements

For the avoidance of doubt, these requirements relate only to the data protection aspects of remote working and is not a general guide on remote working practices.

Staff working remotely must continue to adhere to all relevant University guidance and policies applicable to their work; including ensuring that mandatory training on Data Protection and Information Security is completed annually. In particular, staff must be aware of and comply with the:

- Data Protection Policy; and
- Information Security Policy

Remote working includes working on any digital or hard copy University information off-site. It may involve work from home, at another off-site location including visits to other institutions, or working whilst on the move.

All work data remains the property of the University and may be required at any time.

Under the Data Protection Act, personal data can only be processed off campus if all of the following conditions are met:

- the personal data is used or processed to carry out the duties of the member of staff in support of their role and for no other purpose;
- the processing is carried out only for legitimate purposes related to University business;
- the Data Protection Principles are followed strictly; and
- adequate security is maintained to protect against the loss, theft or unintentional disclosure of the personal data, both digital and physical records.

Storing and transferring documents

Staff are responsible for ensuring the security of University property and University information whilst working remotely.

The transfer of hard copies of documents between the University and a location off campus to work remotely should be avoided. Where possible any such hard copy records should be scanned electronically and stored in a sensible repository e.g. SharePoint, for access offsite. In exceptional circumstances, where hard copy documents are transported and they are confidential/sensitive, then they must be placed in a secure closed envelope/folder and clearly marked private and confidential, with a BCU return address contained on the envelope/folder. Any hard copy records taken off campus must not contain any personal data without the explicit permission of your line manager.

Staff must ensure such documents are kept in their view or in a secure and lockable storage device at all times when off-site. Managers must be informed when staff do transfer hard copy documents off-site and this should be recorded, in writing, within the department. Certain categories of documents may not be permitted to be transported off-site and managers must be consulted on such matters.

Staff should always ensure that the master copy of the record, whether paper or electronic, is not removed from University premises.

Staff must not copy any University information from their University device to a non BCU device; this

includes not emailing information to personal email accounts to access remotely. BCU provides access to laptops and mobile phones where required by staff to enable secure access to BCU information.

Always consider how necessary it is to take personal data off University premises, taking the following into account:

- Rather than storing personal data on a mobile storage device, it may be possible to use SharePoint or OneDrive to access the information remotely. This would remove the need for any personal data to be physically carried off premises and reduce the risk to the University. If you have trouble accessing SharePoint or OneDrive remotely, please speak to IT.
- If you need to use hard copy documents containing personal data, assess whether you need the whole file or whether you could limit the personal data you take off premises to minimise the risk of loss.
- Consider whether personal data can be fully anonymised before being taken off site.
- Specifically avoid taking any physical records off site which include special category data; this must be undertaken only with the express permission of your line manager following a risk assessment. A breach of the Data Protection Act will be deemed more serious if it involves special category data.

Data security whilst working remotely

Equipment and information must be secured whenever it is not in use. You must always lock your screen when not at your machine and, where available, physically lock away any hard copy data. Staff must hide password/lock combinations when typing/entering them; particularly when in an insecure environment, such as during travel on public transport.

Staff must consider the environment around them when working remotely. For example, equipment and screens must be positioned out of sight of others through windows or general view. Devices must also be kept out of sight of any cameras / recording devices (including smart speakers or akin devices), so that the information cannot be overlooked or overheard.

Staff must not work on highly confidential information in public places and will need to relocate to a secure or confidential environment to work on any such matters.

Whenever working remotely on a BCU device staff must utilise the VPN connection provided through the Citrix Gateway where possible.

Staff should always attempt to use a secure internet connection when working remotely (i.e. a private home network - if password protected, or, a secure wireless network run by an institution or organisation they are visiting). Staff should speak to IT if they have any concerns about the security of a connection or the security of the information on their equipment.

Staff must act with care when using public or free wi-fi services (such as those commonly found in public libraries, bars and coffee shops and where they can be joined without a password) and ensure that any sites to which they are directed are the genuine sites and, once browsing is finished, to log off any services and tell the device to forget the network.

Equipment

Staff are advised to only save University data onto their BCU provided laptops and remote working equipment (e.g. staff mobile phones).

University documents must not be saved onto personal devices.

To support secure working when away from BCU staff should use the relevant technology including Microsoft Teams, Outlook and SharePoint.

Staff are only advised to use BCU approved equipment (e.g. BCU encrypted memory sticks) for moving and transferring data between different devices when there is a specified business purpose to do so.

Staff must not use computers owned and managed by a third party i.e., internet café to access BCU systems. Internet cafés are by design much more likely to be infected with malicious software which may attempt to harvest your login credentials or any information you can access.

Working while travelling

Staff must take steps to ensure the environment they are working in offers a suitable level of privacy and need to be vigilant of shoulder surfing (where an individual reads what you are doing over your shoulder or in a gap between seats).

Staff must attempt to avoid holding confidential conversations (whether face to face or via technology) in places where others may overhear the content and should move to a confidential area to discuss such matters; or ask a caller to delay the conversation until the call can be taken in private.

Staff must not leave laptops, mobile phones or any BCU data unattended in a transport vehicle (e.g. car/train, both private and public transport).

Risk management and information security incidents

Even whilst working remotely all security incidents or near misses must be reported promptly to minimise loss and damage to data. Anyone who encounters an information security breach must report it immediately to the IT Help Desk.

If a staff member loses a laptop/mobile device whilst working remotely, then they should contact IT Help Desk as a matter of urgency, so that the network can be protected and the device can be remotely wiped, where that functionality exists.

With regard to personal data (i.e. data relating to an identifiable living individual) any suspected data breach must be reported to the Information Management Team as soon as you become aware of a breach.

Please note that BCU only have 72 hours to review a data breach and consider if there is a requirement to report the incident to the Information Commissioner's Office, dependent on the severity of the incident.

Additional points

Staff working remotely must ensure that any University information is retrievable and can be returned to University on request. Subject access and Freedom of Information Act requests may cover

information held remotely, therefore in the event of a request for information staff must retrieve and return all relevant information promptly.

Limit print outs to information that is not sensitive. Dispose of any printouts by shredding using a cross-cut shredder or return such hard copy records to a BCU site for disposal in confidential waste. For specific IT guidance on the requirements and processes when working remotely, please refer to IT.

Agile Working

The University continues to focus on and develop agile working practices, whereby staff will be able to work in different ways and from different locations. Exceptions to this guidance must be discussed with line managers and reviewed by Information Management or Information Security Teams as appropriate before any alternative data handling approach occurs.

BCU Appropriate Policy Document (on the topic of data protection)

In accordance with the Data Protection Act 2018 (DPA 2018)'s requirement, Birmingham City University has this Appropriate Policy Document (APD). It is required when an organisation processes special category personal data and criminal offence data under certain specified conditions. This document is based on a template APD, produced by The Information Commissioner's Office (ICO).

Where the substantial public interest legal basis is used for these purposes, or the condition for processing employment, social security and social protection data, an APD is required to be in place, demonstrating that these conditions are compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles.

1. Substantial public interest condition of processing

In the following circumstances, Birmingham City University relies on the conditions of processing listed below. The conditions have detailed criteria which should be consulted as needed. Those criteria can be found at Data Protection Act 2018 (legislation.gov.uk) Schedule 1 Part 1 Conditions relating to employment, health and research etc.

- Processing student personal data or student application data. The condition that would apply is Schedule 1 Part 2 (1) the equality of opportunity or treatment.

- Processing student complaints or student disciplinary data. The conditions that would apply would be Schedule 1 Part 2 (1) the equality of opportunity or treatment, Schedule 1 Part 2 (10) Preventing or detecting unlawful acts or Schedule 1 Part 2 (18) Safeguarding of children and individuals at risk.

- Processing student academic appeals or extenuating circumstances data under the activity of student assessment administration. The condition that would apply is Schedule 1 Part 2 (1) the equality of opportunity or treatment condition.

- Processing student special assessment requests under the activity of student assessment administration. The conditions that would apply would Schedule 1 Part 2 (1) the equality of opportunity or treatment, or Schedule 1 Part 2 (16) support for individuals with a particular disability or medical condition.

- Processing student placement data such as tutor and student reviews, reports, evaluation, summaries, handbooks. The conditions that would apply would be Schedule 1 Part 2 (1) the equality of opportunity or treatment, or Schedule 1 Part 2 (18) Safeguarding of children and individuals at risk.

- Processing student data which might include information regarding health to consider and provide advice, support and reasonable adjustments. The conditions that would apply would be Schedule 1 Part 2 (16) Support for individuals with a particular disability or medical condition, or Schedule 1 Part 2 (18) Safeguarding of children and individuals at risk.

- when processing backup data for IT management purposes. The condition that would apply would be Schedule 1 Part 2 (10) Preventing or detecting unlawful acts.

- when providing information to investigative authorities for the purposes of the prevention or detection of crime. The condition that would apply is Schedule 1 Part 2 (10) Preventing or

detecting unlawful acts.

- when processing special category data as part of surveys where the special category data is related to equality of opportunity or treatment. The condition that would apply is Schedule 1 Part 2 (1) Equality of opportunity or treatment.

- When processing special category data and / or criminal offence data in order to provide confidential counselling, advice or similar or of another similar service. The condition that would apply is Schedule 1, Part 2 (17) Counselling.

- When processing any special category and / or criminal offence data in order to protect the physical, mental or emotional well-being of an individual under the age of 18, or over the age of 18 and at risk. The condition that would apply is Schedule 1, Part 2 (18) – Safeguarding of children and individuals at risk

2. Employment, social security and social protection condition of processing

In the following circumstances, Birmingham City University relies on the conditions of processing listed below. Each condition has detailed criteria which should be consulted as needed. Those criteria can be found at Data Protection Act 2018 (legislation.gov.uk) Schedule 1 Part 2 Substantial Public Interests.

- Sharing staff occupational health data with outsourced occupational health providers. The conditions that would apply to this would be Schedule 1 Part 2 (1) the equality of opportunity or treatment, or Schedule 1 Part 2 (16) support for individuals with a particular disability or medical condition.

- Sharing data with regulatory bodies for the purposes of health and safety – this could be staff, student or associate data. The condition that would apply is Schedule 1 Part 2 (12) regulatory requirements.

- Processing accident and incident reports and data, RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations) forms, DSE (display screen equipment) assessments, or eye tests data for the purposes of health and safety monitoring. The condition that would apply is Schedule 1 Part 2 (12) regulatory requirements.

- Processing staff equal opportunities data, for the purposes of job applicant and staff analysis and monitoring. The conditions that would apply to these types of processes would be Schedule 1 Part 2 (1) the equality of opportunity or treatment, and Schedule 1 Part 2 (12) regulatory requirements.

- Processing job applicant personal data, or staff personal data, including staff sickness data and medical certificates; or staff training and development data, or staff appraisal data; or staff grievance or disciplinary data; for the purposes of staff administration or management. The conditions that would apply to these types of processes would be Schedule 1 Part 2 (1) the equality of opportunity or treatment, Schedule 1 Part 2 (12) regulatory requirements, Schedule 1 Part 2 (10) Preventing or detecting unlawful acts, or Schedule 1 Part 2 (18) Safeguarding of children and individuals at risk.

- Processing Student Ambassador information for the purposes of the student ambassador process. The conditions that would apply to these types of processes would be Schedule 1 Part 2 (1) the equality of opportunity or treatment, Schedule 1 Part 2 (10) Preventing or detecting unlawful acts, or Schedule 1 Part 2 (18) Safeguarding of children and individuals at risk.

- Processing student data related to students who are applying for or living in accommodation for which the university provides administrative, safeguarding or health and safety services or has responsibilities. The conditions that would apply to these types of processes would be Schedule 1 Part 2 (1) the equality of opportunity or treatment, Schedule 1 Part 2 (12) regulatory requirements, Schedule 1 Part 2 (10) Preventing or detecting unlawful acts, or Schedule 1 Part 2 (18) Safeguarding of children and individuals at risk.

- Processing criminal offence data to protect members of the public from malpractice, unfitness, incompetence or mismanagement in the administration of a body or organisation. The condition that would apply is Schedule 1, Part 2 (11) – Protecting the public from dishonesty.

- Processing criminal offence data to comply with a requirement which involves taking steps to establish whether an individual has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct. The condition that would apply is Schedule 1, Part 2(12) – Regulatory requirements relating to unlawful acts and dishonesty.

- Processing data to fulfil the University's responsibilities as an educational institution and in particular to provide higher education, carry out any research and publish the results, and to conduct itself in a manner compliant with its responsibilities under the Education Reform Act (3). The condition that would apply is Schedule 1, Part 2 (6) – Statutory and government purposes.

- Complying with any other legal requirements, such as the requirement to disclose information in connection with legal proceedings. The condition that would apply is Schedule 1, Part 2 (6) – Statutory and government purposes.

- Processing data to indemnify itself and its students and staff against any covered losses and to ensure that the University and its members have an appropriate level of protection. The condition that would apply is Schedule 1, Part 2 (20) – Insurance.

- Processing data to fulfil the obligation to provide an occupational pension scheme and determine benefits payable to dependents of pension scheme members. The condition that would apply is Schedule 1, Part 2 (21) – Occupational Pensions.

- Sharing data with elected representatives, such as MPs or local government councillors at the request of their constituents. The condition that would apply is Schedule 1, Part 2 (24) - Disclosure to elected representatives.

Criminal offence data

Birmingham City University may process criminal offence data during the staff and student recruitment process or during the employment of staff or while a student is enrolled and for up to 7 years afterwards, including about students who are applying for or living in accommodation for which the university provides administrative, safeguarding or health and safety services or has responsibilities. The legal bases for this processing are compliance with a legal obligation, and legitimate interests. The reasoning behind this is as follows: in order for the University to comply with safeguarding and safety regulations; to pursue a legitimate interest in ascertaining the suitability of individuals for a staff role; or to ascertain the suitability of students entering professional programmes. The University follows its Students with Criminal Convictions Policy and Procedure, which applies to applicants and students.

Compliance with the requirements of the UK General Data Protection Regulation (UK GDPR)

Article 5 principles

Birmingham City University processes special category data and criminal offence data lawfully, fairly and in a transparent manner. The legal bases for processing are set out in this document; and more information about the purposes for processing the data can be found in the University's privacy notices. We only process the data where we have valid reasons for doing so; we only collect and process the data which is needed for these purposes. We take reasonable steps to ensure the personal data we hold is not incorrect or misleading, and we have processes in place for ensuring that we do not keep personal data for longer than we need it. We have many measures in place for ensuring the appropriate security of the data. We also have the necessary information security and data protection policies, and we regularly review them.