Data Protection & Privacy Policy
V1.3

Document Approval and Version Control

Document Title	Data Protection & Privacy Policy
Prepared by	Department of Governance
Approved by	Information Management Forum (IMF) (20/3/18) Information Governance Committee (IGC) (29/3/18) Executive Board (EB) (4/4/18) Court (10/5/18)
File Location	Z:\Common\Information Compliance\Data Protection\Policy Guidance\DataProtectionPrivacyPolicyV1.2.docx
Publication Location	https://www.gcu.ac.uk/dataprotection/
Related documents	• Information Assurance Charter • Information & Records Management Policy • Information Classification & Handling Policy • Records Retention Schedules • CCTV Policy • Information Security Incident Reporting and Management • Policy on processing of Special Category and Criminal Convictions Data (not approved yet by IGC so can't be included)
Last Review Date	6/2/23
Next Review Date	6/2/24

Version No.	Status	Date Issued	Author	Update Information
V1.0	Approved	11/5/18	Hazel Lauder – Head of Information Compliance	To replace the Data Protection Guidelines V2.2
V1.2	Approved	5/8/20	Updated by Morgan O'Neill, Thorntons	Annual review and update
V.1.3		21/1/23	Updated by Morgan O'Neill Thorntons	

Contents

1. Introduction 4
2. Purpose of this Policy 4
3. Policy Statement 4
4. Scope 4
5. Responsibilities of Staff 4
6. Responsibilities of Students 5
7. Responsibilities of Third Parties Working on Behalf of the University 5
8. Data Protection Principles 5
9. Records of Processing Activities 6
10. Transferring Data Outside the United Kingdom 6
11. Chinese Personal Information Protection Law ('PIPL') 7
12. Legal basis for Processing Personal Data 7
13. Individuals Rights 7
14. Direct Marketing 8
15. Retention & Disposal 8
17. Information Security 8
18. Information Breach Management 9
19. CCTV 9
20. Research 9
Appendix A – Glossary of Terms 10
Appendix B – Data Protection Officer 11
Appendix C – Conditions for Processing Data 12

1. Introduction

1.1 The University needs to process personal data about its employees, workers, students, clients and other individuals for various purposes. These purposes include managing the progress of students, managing staff, recruiting and employing staff ('data subjects') and complying with legal and statutory regulations. Information which relates to a living individual is considered to be 'personal data'.

1.2 The Data Protection legislation including the UK General Data Protection Regulation ('UK GDPR') and Data Protection Act 2018 ('data protection law'), sets out the obligations and responsibilities of organisations which manage personal data. The University has adopted this Policy to ensure compliance with this and any other data protection legislation which applies to GCU.

1.3 This policy is published on the University website and any amendments or revisions will be noted within the document control section.

1.4 A review of this policy is undertaken on an annual basis with content being updated as appropriate. Policies and guidelines may be altered at any time if amendments are deemed necessary.

2. Purpose of this Policy

2.1 This Policy sets out the responsibilities of the University, its staff and its students to comply with the provisions of data protection law. Training, guidance and procedures are in place to support compliance with this policy.

3. Policy Statement

3.1 Glasgow Caledonian University is committed to protecting the rights and freedoms of individuals in respect of processing their personal data.

3.2 The University manages the personal data that it processes in accordance with data protection law and good practice.

3.3 This documents sets out responsibilities and actions that the University takes to meet this commitment.

4. Scope

4.1 This Policy applies to all staff, students and governors of GCU any other people processing date on behalf of GCU. It relates all personal data created, collected, stored and processed through the activity of the University and where the University is the Data Controller. (A Glossary of Terms is provided in Appendix A).

5. Responsibilities of Staff

5.1 The University Secretary has overall responsibility for, and ownership of, the Policy.

5.2 Members of the Executive are responsible for endorsing, implementing and supporting the Policy and any amendments.

5.3 Directors, Deans and Heads of Department are responsible for ensuring that their School/ Department adopt and conform to this Policy.

5.4 The Data Protection Officer (DPO) is responsible for the implementation and management of this Policy. (The details of the DPO are provided in Appendix B).

5.5 The Data Protection Team within Governance and Legal Services are responsible for providing advice and guidance in relation to Data Protection matters and for managing requests made by Data Subjects.

5.6 Other roles within the University support the management and security of information and records including Information Services, IT security and physical security.

5.7 The Information Governance Committee (IGC), Information Management Forum (IMF), and the Data Protection Compliance Leads and Data Protection Compliance Co-ordinators have key information assurance and governance roles.

5.8 All staff must undertake relevant Data Protection and information security training.

5.9 All staff are individually responsible for ensuring that the processing of personal data is in accordance with University policy and guidelines.

6. Responsibilities of Students

6. 1 Students are not permitted to process personal data in connection with their studies without obtaining written approval from an appropriate member of academic staff. Students must obtain approval before processing takes place.

6.2 Students should abide by this Policy, comply with the data protection law, seek guidance and follow the instructions of the University in relation to any uses of personal data.

7. Responsibilities of Third Parties Working on Behalf of the University

7.1 The University is responsible for the processing of personal data by third party companies or individuals working on its behalf.

7.2 Staff who engage any third party who will process personal data on their behalf such as contractors, external supervisors, external examiners, must ensure that these third parties are aware of their responsibilities. This includes managing personal data in accordance with this policy and adhering to its terms, limiting access to only personal data required for the work/activity, returning or destroying personal data on completion when the activity is complete and ensuring that appropriate contractual arrangements are in place with third parties.

8. Data Protection Principles

8.1 To comply with data protection law, the University must operate in accordance with the seven Data Protection Principles set out in UK GDPR

8.2 Compliance with these Principles help the University ensure that personal data is processed fairly and for a legitimate purpose and securely with measures in place to protect the rights of individuals.

The Principles are:

(a) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').

(b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation').

(c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').

(d) Personal data shall be accurate and where necessary kept up to date ('accuracy').

(e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').

(f) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

(g) The University must take responsibility for, and be able to demonstrate compliance with the Data Protection principles. ('accountability').

9. Records of Processing Activities

9.1 Data protection law requires Data Controllers to maintain a record of processing activities (ROPA) which documents the personal data processing activities carried out at the University. The ROPA helps the University demonstrate accountability with data protection law and may be requested by the Information Commissioner.

9.2 The University maintains ROPA within the Information Asset Register (IAR) to capture these requirements which include: the purpose of the processing, the types of individuals about which personal data is held, who the personal data is shared with and when personal data is transferred to countries outside the UK.

10.Transferring Data Outside the United Kingdom

10.1 Personal data can only be transferred out of the United Kingdom to third countries under certain circumstances ('Restricted Transfer').

10.2 The University has guidelines to ensure that an adequate level of protection is provided for the personal data. This includes an assessment of information security arrangements and implementing contracts and/or Data Processing Agreements with third parties.

10.3 Any agreements or contracts concluded concerning data that are transferred outside of the UK to a country which is not covered by an 'Adequacy Decision' should be accompanied by an 'International Data Transfer Agreement' ('IDTA').

10.4 Colleagues should seek advice from the Data Protection team before concluding new data processing agreements, or updating existing contracts, where a restricted transfer is involved.

10.5 It may be necessary to complete a Data Protection Impact Assessment ('DPIA') and a Transfer Impact Assessment to document and review the risks associated with the restricted transfer. Please seek advice from dataprotection@gcu.ac.uk

11.Chinese Personal Information Protection Law ('PIPL')

11.1 The PIPL is the data privacy law in China. This law has extra-territorial scope which means that is can apply to the processing of personal data about Chinese citizens outside the UK. When GCU processes personal data about students or University colleagues in China, it must comply with some aspects of this law.

11.2 When concluding any contract, or updating existing contracts that relate to the processing of the personal data of individuals in China, for example, during the application process GCU must ensure that contracts concluded include a data processing agreement, which incorporates the IDTA and describes the security measures GCU will put in place to protect the personal data.

11.3 The University must ensure transparency in relation to processing and be clear on the lawful basis for processing data. Colleagues should seek advice from the Data Protection team if they are unsure whether the provisions of PIPL apply, or if any additional safeguards are required when concluding or updating contracts concerning the personal data of Chinese student applicants in China.

12.Legal basis for Processing Personal Data

12.1 The University will ensure that there is a legal basis to process personal data and special categories of personal data. The legal basis should be recorded in the IAR. (The conditions for lawful processing are provided in Appendix C). The University has a separate policy on processing Special Category and Criminal Convictions Data.

13.Individuals Rights

13.1 The University has procedures and guidance to ensure that arrangements are made to provide for the rights available to data subjects under data protection law:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.

- Rights in relation to automated decision making and profiling.

13.2 In recognition of the need to protect the rights of children the University takes steps, when processing their personal data, to address their rights and the Data Protection Principles, in particular fairness.

14.Direct Marketing

14.1 The University will comply with the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) when undertaking direct marketing via telephone, text and email.

14.2 The University will ensure that has an appropriate lawful basis to process personal data for marketing purposes. A data subject may request that the University ceases to use their personal data for marketing purposes at any time.

15.Retention & Disposal

15.1 The University has implemented procedures to retain personal data for the length of time the data is required for the specific purpose for which it was collected.

15.2 The length of time that personal data should be retained is outlined in the Records Retention Schedules and these retention periods will be based on legal, business requirements and practice within Higher Education.

15.3 Certain personal data will be retained permanently by the University as part of the University archive.

16.Data Protection by Design and Default

16.1 Data protection law requires the University to integrate appropriate technical and organisational measures to protect personal data and the rights of individuals. This approach to protecting personal data is called 'data protection by design and default'. This includes implementing measures to ensure that privacy and the protection of personal data is considered during the design stage of a process and to use appropriate technical and organisational measures to minimise the risk to personal data.

16.2 This can be achieved through the completion of Data Protection Impact Assessments (DPIAs). DPIAs are a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce privacy risks.

16.3 To reduce the risks associated with handling personal data techniques such as pseudonymisation and anonymisation will be implemented.

17.Information Security

17.1 The University has policies and guidelines to ensure that staff and students meet their responsibilities relating to ensuring that:

- Any personal data which they hold is kept securely, protecting the confidentiality, integrity and availability of information.

- Personal data is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

18.Information Incident Management

18.1 Information Incident Management policies and processes are in place to record personal data breaches and enable personal data breaches to be reported. Procedures ensure that the University is able to report any personal data breach which is likely to result in a risk to the rights and freedoms of Data Subjects to the Information Commissioner's Office within 72 hours of becoming aware of the personal data breach.

19.CCTV

19.1 CCTV is used for the purposes of the prevention of crime and to protect public safety and the security of the University community. CCTV footage may be used for investigations or proceedings arising under the University's regulations, codes and policies. The University has a separate CCTV policy in place.

20.Research

20.1 The process for approval of research projects involving human participants will address the requirements of data protection law in relation to data subject rights and privacy.

Appendix A – Glossary of Terms

Adequacy Decision	A decision by the UK government that certain countries provide adequate safeguards for personal data protection. An IDTA is not required for data transferred to a country under an adequacy decision. This includes EU/EEA Member States, among others.
Anonymisation	The process of turning personal data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the personal data.
Automatic decision-	Making a decision solely by automated means without any human involvement.
Data Controller	Natural or legal person, public authority, agency or other body who determines the purposes and means of processing personal data.
Data Processor	Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Impact Assessment (DPIA)	A process which can help organisations identify the most effective way to comply with their data protection law. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.
Data Subject	Identified or identifiable natural living person.
Direct Marketing	The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This covers all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations for example, it covers a charity or political party campaigning for support or funds.
IDTA	International Data Transfer Agreement
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	Automated processing of personal data to evaluate certain things about an individual.
Pseudonymisation	Procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers or pseudonyms.
Restricted Transfer	A transfer of data to a third country outside the UK which requires additional safeguards such as an Adequacy Decision or an IDTA to comply with the UK GDPR
Special Categories of Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Information relating to criminal convictions and offences are not included but should be offered the same level of protection.
Staff	Staff includes employees, casual workers and any other individual temporarily fulfilling a role normally held by a member of staff (e.g. agency worker, self-employed contractor).

Third Country	Country outside the UK.

Appendix B – Data Protection Officer

The contact details are:

Data Protection Officer (DPO)
Department of Governance
Glasgow Caledonian University
Cowcaddens Road
Glasgow
G4 0BA

Email: dataprotection@gcu.ac.uk

Telephone: 0141 331 8392

Appendix C – Conditions for Processing Data

Conditions for Processing Personal Data (Article 6 (1), UK GDPR)

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party; except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject; which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Conditions for Processing Special Categories of Data (Article 9 (2), UK GDPR)

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy domestic law;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.