BROOKDALE COMMUNITY COLLEGE
COLLEGE REGULATION

4.7005R General Data Processing Regulation (GDPR) Regulation

I. Title of Regulation

General Data Processing Regulation (GDPR) Regulation

II. Objective of Regulation

This Regulation outlines the College's application of GDPR requirements.

III. Authority

Board of Trustees Bylaw 1.3054; Policy 4.7002 Information Security Program; EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

IV. Regulation Statement

The objective of this Regulation is to outline Brookdale Community College's (the "College") administrative, technical, and physical information safeguards mandated by the General Data Processing Regulation ("GDPR").

The European Union (E.U.) adopted the GDPR on 27 April 2016 which sets in place new data protection and compliance standards that seek to unify and strengthen data usage practices and protections for all individuals that reside in the E.U. It also aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by centralizing the regulation within the E.U. Since the scope of these protections is very broad and encompasses any export of personal data outside the E.U., the GDPR has widespread effects throughout education institutions around the globe. In order to safeguard E.U. citizens from data breaches, the GDPR requires that any organizations or institutions (within or outside of the E.U.) that process or hold personal data of citizens residing in the E.U. be compliant with the new standards. The GDPR became enforceable on 25 May 2018.

This Regulation, together with Brookdale Community College's ("the College") written Information Security Program ("the InfoSec Program") Policy (Policy 4.7002) and accompanying Regulation (4.7002R) addresses information safeguards mandated by the GDPR.

1. Applicability

The GDPR standards apply to the obtaining, processing, storing, and security of any record that contains non-public personally identifiable information about a student or other third party who has a relationship with the College, whether in paper, electronic, or other form, which is handled or maintained by the College or on behalf of the College or its affiliates. For the purposes of this Regulation, non-public personally identifiable information (PII) is further explained and governed under the four levels of data classification defined by the College's Data Classification and Permitted Use Regulation (4.7003R).

2. Key Definitions

2.1 The GDPR defines a '***data subject***' as: "identified or identifiable natural person[s] who reside[s] in the E.U." The intentional breadth of this definition implies that regardless of whether or not an individual is an E.U. citizen or permanent resident the GDPR will apply to their information. For instance, the GDPR requirements would also apply to American students or faculty members who communicate with campuses while they are in Europe.

2.2 Under the new standard '***personal data***' is defined as: "any information relating to an individual [i.e. '***data subject***'], whether it relates to his or her private, professional, or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

2.3 The GDPR defines '***data controllers***' as: "the natural or legal person, public authority, agency, or another body which, alone or jointly with others, determines the purposes and means of the processing of ***personal data***." '***Data controllers***' are those persons or groups that make decisions about ***personal data*** processing.

2.4 The GDPR defines '***data processors***' as: those entities that process ***personal data*** on behalf of ***data controllers***, and as directed by ***data controllers*** of ***personal data***." '***Data processors***' are those persons or groups to whom ***data controllers*** have delegated or outsourced ***personal data*** processing activities.

3. Roles and Responsibilities

3.1 Responsibilities: The College's Vice President of Finance and Operations (VPFO) and Chief Information Officer (CIO) are responsible for coordinating and overseeing the College's InfoSec Program; implementing GDPR compliance is a component of that program.

3.2 Risk Identification, Assessment, and Compliance: As part of the College's written InfoSec Program Regulation, the College will identify and assess external and internal risks to the security, confidentiality, and integrity of non-public PII. This identification and assessment includes:

- ***Audits:*** On a routine basis, the College will perform audits for areas affected by the GDPR to understand, identify, and classify what data the

College holds, where that data is stored, how that data is used, and to assess associated risks. Current and new types of PII will be identified and handled as a routine and recurring aspect of these audits. The CIO will work with departments on any items that need remediation.

- ***Data Governance, Policies, and Consent:*** On a routine basis, the College will review its data governance policies that regulate the gathering, handling, and storage of ***personal data***. The College will also work with staff members who are defined as ***data controllers*** or ***data processors*** to review the consent, privacy, right-of-access, communication, and documentation processes for the various levels of PII that the College retains. During routine governance reviews, the College will strive to refine, improve, and streamline its process to accommodate requests from ***data subjects*** to retrieve, correct, or erase/anonymize (whenever one of the two is appropriate, possible, and legally permissible) their data. The CIO will work with departments on any items that need further measures or remediation.

- ***Data Protection and Security:*** On a routine basis, the College will review its data protection and security measures related to processing, usage, storage, and backup of records containing ***personal data***. To protect and secure ***personal data***, the College will continually aim at either the encryption, pseudonymization, or anonymization of records containing sensitive PII (as defined in the College's Data Classification and Permitted Use Regulation, 4.7003R) whenever possible, legal, and appropriate. The College will also design and deploy data protection procedures to be implemented or utilized in the relevant conditions and to further support a data-protection-by-design approach to PII handling.

- ***Employee Training and Management:*** In addition to the general information security training that all staff members are required to review on a yearly basis, staff members at the College who are defined as ***data controllers*** or ***data processors*** will also be required to review the College's GDPR Regulation, GLBA Regulation, Release of Academic and Demographic Data About Students Regulation ("FERPA," 6.1504R), and any departmental procedures pertaining to GDPR, GLBA, or FERPA. Annual certification of department compliance will be provided by the appropriate department heads to the VPFO and CIO.

- ***Information Systems and Detecting, Preventing, and Responding to Attacks:*** The College will identity reasonably foreseeable risks to Information Systems and address detection, prevention, and responding to attacks through the procedures outlined in the College's written Information Security Program Regulation (4.7002R). The College will also implement tools and set procedures in place to detect, report, and investigate any breach of ***personal data***.

3.3 Designing and Implementing Safeguards: The CIO will work with departments to implement safeguards to control the risks identified through the audits, governance reviews, or data protection procedures mentioned above.

3.4 Overseeing Service Providers: As part of the College's third-party Institutional Data safeguarding process, and under the direction of the VPFO, all service providers that handle, store, transmit, or receive Institutional Data must incorporate language into the College's contracts stating that the service provider will protect the College's Institutional Data according to commercially acceptable standards and no less rigorously than it protects its own data. For service providers or vendors that provide Software-As-A-Service solutions (hosted solutions) and handle, store, transmit, or receive Institutional Data, the College also requires inclusion of an InfoSec contract clause which will be reviewed by the Executive Associate Legal Services, the CIO, and the VPFO.

3.5 Adjustments: The VPFO and the CIO are responsible for evaluating and adjusting the GDPR Regulation based on the risk identification and assessment activities undertaken, as well as any material changes to the College's operations or other circumstances that may have a material impact upon it.

4. Review Cycle

This Regulation will be reviewed and updated as needed, at least annually.

5. Compliance and Enforcement

As described in the InfoSec Program Regulation (4.7002R), whenever a faculty member, staff member, contractor, student, or third-party is found to be negligent in, or have a blatant disregard for, the compliance with the InfoSec Program Policy or an approved security compliance standard, the College's first recourse will be in training the offender. Additional infractions will incur progressive discipline. The College reserves the right, however, to consider certain single incidents of non-compliance to be so harmful as to immediately rise to the level of more serious disciplinary consequences, up to and including a long term suspension of employment, termination of employment, removal of service, academic suspension, academic expulsion, termination of third-party relationship, or termination of contract.

IV. Responsibility for Implementation

The President.

The VPFO and CIO are responsible for monitoring compliance with this Regulation and reporting instances of non-compliance to the College's Senior Leadership Team stakeholders.

Related Policy; https://www.brookdalecc.edu/about/board-of-trustees/college-policies/4-0000-business-finance/4-7002-information-security-program/

Approved by Brookdale's Data Standards and Information Security IT Governance Committee on 9/9/2020

Approved by Brookdale's Information Technology Steering Committee on 10/8/2020

Approved by the Senior Executive Leadership Team on 1/6/2021

Approved: President, 1/6/2021