Purpose	Electronic resources are the property of BPP Institute and intended for carrying out the business operations of BPP Institute, and to support students' teaching and learning activities. This policy clarifies the obligations and expectations regarding the use of electronic resources made available by BPP Institute to its students, staff, and related personnel. This policy is subject to and in accordance with all applicable national, regional, or local laws and regulations, concerning privacy and data protection.
Scope	This policy applies to all students, staff, independent contractors, consultants, and external board and committee members.
Policy Principles	**1. General** 1.1. BPP Institute resources include all technical, electronic and communication systems and resources provided to support BPP Institute business operations and for students' usage in teaching and learning activities. 1.2. These resources include those that are owned, leased or otherwise controlled by BPP Institute, that are used or accessed from BPP Institute premises or other remote locations, or that are used for BPP Institute business, including all hard/paper copies of any communication derived from Electronic Resources. 1.3. These resources include but are not limited to: a. desktops and portable computer systems b. telephones, wireless devices, mobiles, tablets c. internet and web access, voicemail, e-mail, electronic chat rooms, apps d. media storage devices, equipment, and systems. This policy also applies to all activities using any BPP Institute paid accounts, subscriptions, or other technical services, such as internet and web access, voicemail, and email, whether or not the activities are conducted from company premises. 1.4. The user must ensure usage of BPP Institute electronic resources in a lawful, ethical, and responsible manner. 1.5. Only persons with proper authorisation by BPP Institute IT support services are allowed to use BPP Institute electronic resources. 1.6. All users are required to use BPP Institute electronic resources responsibly and not cause unnecessary damage or disruption to the resources and/or services. **2. Unacceptable Use**

2.1. Users may not use BPP Institute electronic resources for personal use in a manner that interferes with work or any responsibilities to students, staff, or related personnel.

2.2. Use of BPP Institute electronic resources to conduct a user's personal business enterprise, for personal gain, or the advancement of individual views is prohibited.

2.3. Viewing, sending, or saving offensive material is strictly prohibited. Offensive material includes, but is not limited to, pornography, sexual comments, racial slurs, gender-specific comments, jokes or images that would offend someone on the basis of their race, colour, creed, sex, age, religion, national origin, or ancestry, physical or mental disability, veteran status, as well as any other category protected by national, state or local laws and regulations.

2.4. Users who engage in unacceptable uses of electronic resources may be subject to disciplinary action (see Section 7 Compliance).

3. Acceptable Use

3.1. Limited and reasonable personal use of electronic resources by users will be deemed acceptable if the use:

a. does not violate any applicable law, regulation, or BPP Institute policy
b. does not add unreasonable incremental expense to BPP Institute
c. in no way damages BPP Institute`s good name, or reputation, or result in, or place BPP Institute at risk of incurring any liability
d. in no way affects the operation, availability or performance of BPP Institute's information and technology systems
e. does not interfere with the performance of the user's duties for BPP Institute; and
f. does not interfere with the users' productivity or the productivity of any other user(s).

4. Blocking and Monitoring

4.1. BPP Institute expressly reserves the right to block and/or monitor or review all information and communications that are viewed, created, sent, or retrieved over BPP Institute electronic resources, as may be required to prevent illegal or unethical activities or as may be otherwise required to protect BPP Institute's legitimate business interest.

4.2. Users should not presume that all such information or

communications would be considered private and confidential. All information, including text and images, may be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

5. Ownership of Content

5.1. Subject to any applicable laws, licences and agreements, all information, communications and data maintained on any BPP Institute owned or operated equipment, or any communication system wherever located, is the property of BPP Institute and not the person originating or storing the communications or data.

6. Passwords and Login Information

6.1. It is the responsibility of students, staff, and related personnel to protect their login information and passwords.

6.2. Users of BPP Institute electronic resources are not to share login information or passwords with other users.

6.3. All users must ensure that they log off from computers that are no longer in use, or ensure the screen is locked if away from the computer for any period.

6.4. ***Multi-Factored Authentication (MFA)***

To enhance the security of its IT environment, and in alignment with IT security measures implemented at BPP Education Group, BPP Institute has implemented MFA requiring the user to provide two verification factors to gain access to a resource such as an application or account. In addition to the traditional username and password, MFA requires an additional verification factor which decreases the likelihood of a successful cyber-attack.

Simultaneous with the creation of an account for a new employee, the MFA security feature will be enforced. When the new user logs on for the first time, they will be prompted to provide an additional means of identification, e.g. a mobile phone number. The application will send a verification code to the nominated source which the user has to provide prior to the application giving the user access.

The MFA security feature is applicable to all users within BPP Institute.

7. Compliance

7.1. Failure to comply with this Policy, Standards and Guidelines will

	subject the offending party to disciplinary action, up to and including termination of the staff employment relationship, business contractual relationship and /or legal action, in accordance with all applicable laws and regulations. 7.2. If students fail to adhere to this policy, lecturers, at their discretion, may issue a verbal warning to the offending party at the first instance of breach; and formal written warnings may be issued for subsequent or repeated offences. a. Depending on the severity of the offence (assessed on a case-by-case basis), the Dean may subject the offending student, to any disciplinary action as he/she deems fit. BPP Institute reserves the right to suspend, revoke, or restrict their access of electronic resources; and in severe cases, suspend or terminate their enrolment at BPP Institute.
Related Documents	Anti-Corruption, Bribery and Fraud Prevention Policy BPP Institute Employment Terms and Conditions Copyright Act 1968 (Cth) Cybercrime Act 2001 (Cth) Defamation Act 2005 (Vic) Freedom of Information Act 1982 (Vic) Intellectual Property Policy Privacy Act 1988 (Cth) Privacy and Personal Information Policy Privacy and Personal Information Procedure Staff Code of Conduct Student Code of Conduct Policy Student Code of Conduct Procedure Telecommunications (Interception and Access) Act 1979 (Cth)
For Administrative Use Only	
Responsible Officer	Chief Executive Officer
Contact Officer/s	Chief Executive Officer Dean
Approved by	Board of Directors
Definitions	See BPP Institute`s Glossary of Terms and Acronyms

Version History		
Version No.	**Approval Date**	**Amendment/s**
1.	May 2025	First iteration • For BPP Institute