Procedure	The Electronic Resources Use Procedure provides standards and guidelines that should be read in conjunction with the Electronic Resources Use Policy. This Procedure operationalises relevant elements of the Policy and details processes for adherence. **1. Standards for the Use of Electronic Resources** 1.1. Copying or distribution of copyrighted information is forbidden. This includes the use of any BPP Institute Electronic Resource to obtain, store or share media such as music, movies, or software. 1.2. Electronically changing a User's identity when using any BPP Institute resource is strictly prohibited. 1.3. Passwords issued individually to each employee or associate are intended to apply only to the authorised User. Password sharing is generally prohibited to protect other employees from inappropriate suspicion in the event that an account is used for inappropriate purposes. Prior approval must be sought from the Chief Executive Officer (CEO) if two or more employees need to share a password to access a shared mailbox account or third-party software in order to perform their operational duties. 1.4. Installation of peer-to-peer software or similar file sharing programs on any BPP Institute computer without a specific business purpose or approval is prohibited. 1.5. Chain letters of any kind are not to be sent to or from BPP Institute equipment without the approval of the CEO. 1.6. Employees are to ensure they store master copies of their work data on the Company's intranet (SharePoint) or in their Institution/Function/Project Team's permitted shared drives and systems (such as OneDrive) and not solely on their PC's or laptop local drive or other storage media. Otherwise the data will not be backed up and is at risk of loss or data integrity breach. 1.7. Removable media storage of any type including but not limited to USB flash drive, removable fixed drives, should not be used by employees, without prior approval of the CEO for special circumstances. Removable media is personal and portable which introduces risk into our organization whenever it is used to store sensitive, confidential and proprietary information. Aside from the chance of loss and theft, removable media format storage is a known source of malware infections. 1.8. Employees should seek advice and assistance from the CEO if they need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring our network to a standstill.

The CEO may seek advice from the Director – Operations if special arrangements are needed to manage large files.

2. Electronic Resources User Guidelines

2.1. Every communication sent using a BPP Institute Electronic Resource is identified as originating from BPP Institute or its related entity and carries the BPP Institute name. When using Electronic Resources each individual should remember that in doing so they are representing BPP Institute and should make sure that the interaction reflects well on BPP Institute.

2.2. Appropriate business language should be used in all communications. In a culturally diverse environment, the use of slang or sarcasm may not be correctly interpreted.

2.3. E-mail is essentially no different from a written document. A file can be stored in the system indefinitely and can be discovered in litigation. Therefore, e-mail messages should be treated as carefully as any written document. Always assume that people other than the intended addressee may see e-mail messages. Once a message has been sent, there is no control over to whom it may be forwarded.

2.4. Do not type your message in ALL-UPPERCASE – this is equivalent to yelling and can be extremely difficult to read (although a short stretch of uppercase may serve to emphasize a point heavily).

2.5. Avoid using "group reply" (reply all) functions whenever possible. The vast majority of messages that receive group replies each day do not warrant them. Abuse of this function generates an enormous amount of unwanted and unnecessary mail: always consider carefully whether a group reply is really required before using it. In most cases replying to the Sender alone is your best course of action.

2.6. Only use Cc: when it is important for those you Cc: to know about the contents of the email. Overuse can cause your emails to be ignored.

2.7. Be extremely careful when you forward e-mails, read the previous e-mail exchanges carefully prior to forwarding the e-mail as it may contain confidential or sensitive information which may have serious consequences for BPP Institute.

2.8. Pay careful attention to where your reply is going to end up: it can be embarrassing for you if a personal message ends up on a mailing list, and it can be bothersome for the other list members.

3. Mobile Phones – Acceptable Usage

3.1. If you are provided with a BPP Institute mobile phone, it is intended to improve work efficiency and timeliness of response for the user and other staff contacting and working with the user. In general, mobile phones should be used for business calls and the length of call should be limited.

3.2. It is recognised that some private calls will occur. These calls should be of short duration and should not interfere with work productivity.

3.3. Users are not to use mobile phones for the following purposes:

a. International calls.
b. Excessive usage. Excessive private calls made from a mobile phone are to be reimbursed by the employee.
c. Sending of images not related to BPP Institute business.
d. Excessive internet browsing.
e. Avoid connecting to the internet via personal hotspot for long periods.

3.4. In determining what might constitute excessive usage, the following guideline is to be used:

- Total monthly data usage exceeding 10 GB

4. Mobile Phones – Handling of Accounts/Reimbursements

4.1. Mobile phone accounts will be reviewed by the CEO on a regular basis. High levels of usage will be identified and taken up with the user.

4.2. In the event of excessive private use, the User must reimburse BPP Institute with an amount equal to the amount which the usage exceeds the cost as per above. The reimbursement should be made within 2 weeks of the User receiving the notification from Finance through their immediate Manager.

5. Safety and Security with Mobile Devices

5.1 Keeping Mobile Devices Secure

The following must be observed when handling company-issued mobile computing devices (such as notebooks and iPads):

a. Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle even if the vehicle is locked. Wherever possible they should be kept on the person or securely stowed.
b. Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended.

	c. Mobile devices should be carried as hand luggage when travelling by aircraft. 5.2 Personal Safety when Using Mobile Phones As the effects of electronic radiation on the human body are at this point in time unknown, BPP Institute recommends: a. Keeping conversations on mobile phones as short as possible. b. Using a standard fix phone or internet-based system (e.g. Skype or MS Teams) where possible. c. Using hands free devices – earpieces. d. **Do not use** a mobile phone while: i. Driving a vehicle without a hands-free device. BPP INSTITUTE will not be held responsible for any legal matters arising from illegal usage of mobile phones, even if it occurred during office hours whilst performing duties for BPP Institute. ii. Refuelling a motor vehicle. On an aircraft, unless permitted during taxiing and announced by the Airline.
Related Documents	Anti-Corruption, Bribery and Fraud Prevention Policy BPP INSTITUTE Confidentiality 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	Dean
Contact Officer/s	Chief Executive Officer Dean

Approved by	Chief Executive Officer
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