POLICY:	COMPUTER USAGE
NVR Ref:	**Standard 2**
IBI Ref:	**IBI-3-C 3**
Statement	All staff members using Computer Resources must comply with the IBI's Computer Usage Policy. 1. Access to confidential resources or any account not belonging to the specific staff member on any computer system owned and operated by is not permitted. 2. Assisting others who are not authorised to gain access to such resources or accounts is not permitted. 3. Staff members may not access or copy directories, programs, files, data, or documents that do not belong to them unless they have permission from the account holder / owner to do so. 4. Except with the prior written permission of the CEO, resources must not be used for commercial purposes or monetary gain. 5. The Institute reserves the right to hold a staff member financially liable if, through negligence or deliberate action, resources are compromised in any way by a staff member. 6. Staff members are prohibited from disclosing passwords to any individuals, except to authorised personnel, and must safeguard their account and its contents, and will be held responsible for any misuse. You may not search for, access, copy, or use passwords belonging to any other staff members. 7. Staff members may not use resources to misrepresent themselves as another individual. If you are a victim of such misrepresentation, you must immediately upon discovery of the incident report the incident to the CEO. 8. Staff members must have written permission from the CEO to remove or copy any resource owned or licensed by the Institute.

Statement (cont)	9. Staff members may not use resources to send, forward, or otherwise disseminate nuisance messages. 10. Staff members may not use resources in connection with activities prohibited by any applicable Institute policy or by any applicable laws, ordinances, rules, regulations, or orders of any public authority having jurisdiction including, without limitation, those concerning trademark, copyright and other intellectual property, unauthorised use of a person's image, civil rights, commerce, computer usage, conspiracy, telecommunications, defamation, forgery, obscenity, and privacy laws. 11. Email and other computer files can never be considered strictly private and confidential, due to: i) The open nature of the Internet and related technology ii) The ease with which files may be accessed, copied, and distributed. Staff members are advised to avoid sending messages by email and storing information in computer files that are of a confidential or extremely personal nature (including, but not limited to credit card or tax file numbers).
References	

VERSION CONTROL

Review/ amendment history

Policy Approved by: Chief Executive Officer

Responsible Officer: Chief Executive Officer

Next Policy Review Date July 2018

Version	Date	Details
1.0	July 2014	Policy issued
2.0	Dec 2014	Updated to reflect Standards for Registered Training Organisations (RTOs) 2015
3.0	April 2015	Updated to reflect NVR 2015 Standards
4.0	April 2016	No material changes
5.0	April 2017	No material change
6.0	August 2017	NO material change