CHEEKS BEAUTY ACADEMY INFORMATION SECURITY POLICY

Policy Statement

Information is a vital asset and requires protection from unauthorized access, modification, disclosure, or destruction. Maintaining the security, confidentiality, integrity, and availability of information stored in the electronic systems and in paper form is a responsibility shared by all users. Violations of this policy may result in disciplinary action up to and including termination.

Policy/Procedures

Users of the organization's systems, both electronic and physical, are responsible for protecting the information processed, stored or transmitted using these resources, and for incorporating the following industry standard best practices into their daily activities.

A. Protecting Confidential Information

1. DO NOT distribute confidential or sensitive data to external entities unless approved by the appropriate authority.
2. Only distribute confidential information to internal entities on a need-to-know basis.
3. Assume all student information is private unless the student has signed a FERPA release form.
4. Use secure means to transmit confidential data.

B. Securing Physical Space/Data

6. Physical spaces such as filing cabinets, offices and workrooms containing protected information shall remain locked when unsupervised.

C. Securing Information on Workstations and Other Electronic Systems

7. Utilize strong passwords to minimize the risk of a password being compromised and data being lost due to unauthorized access.
8. Do not share account names and passwords if the account was not configured to be a shared account.
9. DO NOT open attachments and links embedded in emails unless you are confident the email is from a reliable source and intended to be sent from that source.
10. Log out of public systems when finished working.
11. DO NOT save passwords in web browsers or e-mail clients when using a public computer system.

12. DO NOT post material on any publicly accessible computer or website unless first approved by the appropriate authority.
13. DO NOT intentionally damage, alter, or misuse any business-owned or maintained hardware, software, or information.
14. Secure devices by requiring a password when the device is turned on and when the screen saver is deactivated.
15. All computers (desktops/laptops) accessing electronic data must run up-to-date anti-virus/malware software.
16. Keep all computer systems up to date with the latest software maintenance releases.

D. Communicating Security and Confidentiality Issues

21. Notify administration immediately if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed.
22. Notify administration if sensitive or critical information is lost or disclosed to unauthorized parties, if any unauthorized use of systems has taken place, or if there is suspicion of such loss, disclosure, or unauthorized use.
23. DO NOT discuss information security-related incidents with individuals outside of the organization, or with those inside the organization who do not have a need to know.

Definitions

Confidential Data: Confidential Data is information protected by statutes, regulations, organizational policies, or contractual language. Managers may also designate data as Confidential. By way of illustration only, some examples of Confidential Data include: • Social Security Numbers • Medical records • Bank account numbers • Student records and other non-public student data.

If you have questions regarding whether a specific piece of information is considered confidential, please contact the administration office responsible for that data.