POLICIES AND PROCEDURES DOCUMENT				
DOCUMENT TITLE: Social Media Policy				
This Document is Relevant for:	**DENTAL** ☑	**EARLY YEARS** ☑	**FUNCTIONAL SKILLS** ☑	**ADMIN** ☑
Document Author: **JOHN Turner**				
Is this policy document new or revised / or has minor amendments? **If Yes, please state the reason for the amendments?**				
VERSION NUMBER : ***(if applicable)*** V3 – April 2025 V2 – January 2024				
Associated Documents:				
Date of Approval: **April 2025**		**Review Date:** April 2026		
SIGNED OFF BY: **NAME: John Turner** **SIGNATURE:**				

Social Media Policy

1. This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

2. It applies to the use of social media for both business and personal purposes, whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to Employees.

3. Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of Employee suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

4. Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Personnel responsible for implementing the policy

1. Our Management has overall responsibility for the effective operation of this policy in conjunction with IT Support to ensure it is adhered to.

2. All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all Employees understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

3. All Employees are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to People Services. Questions regarding the content or application of this policy should be directed to People Services or your line manager at first instance.

4. Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

a) breach our obligations with respect to the rules of relevant regulatory bodies;
b) breach any obligations they may have relating to confidentiality;
c) breach our Disciplinary Rules;

d) defame or disparage the organisation or its affiliates, learners, clients, business partners, suppliers, vendors or other stakeholders;
e) harass or bully other Employee in any way;
f) unlawfully discriminate against other Employee or third parties;
g) breach our Data Protection Policy (for example, never disclose personal information about a colleague online);
h) breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

5. Employees should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

6. Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Personal use of social media

1. Personal use of social media is never permitted during working hours or by means of our computers, networks and other IT resources and communications systems, other than in the exceptional cases detailed in our Communications and IT Policy.

2. The organisation understands that employees may wish to use their own devices to access social media while they are at work. Employees must limit their use of social media on their own equipment to their official rest breaks such as their lunch break, times when they are between appointments or times when they are not on the site where they are working.

Monitoring

1. The contents of our IT resources and communications systems are our property. Therefore, Employee should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

2. We reserve the right to monitor, intercept and review, without further notice, Employee activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such.

Resources and systems.

1. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

2. We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

3. Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

Recruitment

1. We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

Responsible use of social media

1. The following sections of the policy provide Employees with common-sense guidelines and recommendations for using social media responsibly and safely.

2. Protecting our business reputation:

a) Employees must not post disparaging or defamatory statements about:
   (i) our organisation;
   (ii) our students or their families;
   (iii) our clients;
   (iv) suppliers and vendors; and
   (v) other affiliates and stakeholders

b) Employees should make it clear in social media postings that they are speaking on their own behalf. Write in the first person and use a personal e-mail address when communicating via social media.

c) Employees are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the masses (including the organisation itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

d) Other than where requested, you must not disclose your affiliation as an employee of our organisation.

e) Avoid posting comments about sensitive business-related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.

f) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your line manager and/or People Services.

g) If you see content in social media that disparages or reflects poorly on our organisation or our stakeholders, you should contact your manager and/or People Services. All Employees are responsible for protecting our business reputation.

7. Respecting intellectual property and confidential information:

a. Employees should not do anything to jeopardise our valuable trade secrets and other confidential information and intellectual property through the use of social media.

b. In addition, Employees should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the organisation, as well as the individual author.

c. Do not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.

d. To protect yourself and the organisation against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Business Development Director before making the communication.

e. The contact details of business contacts made during the course of your employment are regarded as our confidential information, and as such you will be required to delete all such details from your personal social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

8. Respecting colleagues, students, clients, partners and suppliers:

a)

a. Do not post anything that your colleagues or our students, clients, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

b. Do not post anything related to your colleagues or our students, clients, business partners, suppliers, vendors or other stakeholders without their written permission.

This policy sits in line with the GDC Professionalism and Fitness to Practise standards for the dental team, and must be adhered to by all parties involved in the training programme.

Internal concerns must be reported to the Senior Business Manager;
John Turner

John@Asatraining.co.uk
01604 871340

External concerns must be reported to either;
NEBDN
info@nebdn.org

GDC
020 7167 6000