Digital and Social Media Policy.

First Published:	16/10/2020	Originally Created by:	DO
Person Responsible for Policy:	Enable CEO		

Date of Review	Reviewed by	Policy changes	Approved by	Date of next review
16/10/2020	SMT & Admin Lead		SMT & Admin Lead	16/10/2021

Policy Statement:

Enable recognises that the internet provides opportunities to participate in interactive discussions, engage with the wider community, and share information on topics using a variety of social media, such as Facebook, Twitter, blogs and LinkedIn. However, employees' use of social media can pose risks to Enable's confidential and proprietary information, reputation, and can jeopardise the company's compliance with legal obligations.

To minimise these risks, to avoid loss of productivity and to ensure that Enable's IT resources and communications systems are used only for appropriate business purposes, we expect employees to adhere to this policy, which outlines staff responsibilities when accessing and using social media websites.

Who is covered by the policy:

This policy covers all individuals working at all levels, including full time and part-time employees, fixed-term employees, consultants, contractors (collectively referred to as staff in this policy). Third parties who have access to Enables electronic communication systems and equipment are also required to comply with this policy.

Scope and purpose of the policy:

This policy deals with the use of all forms of social media, including but not limited to, Facebook, LinkedIn, Twitter and all other social networking sites, and all other internet postings, including blogs. Enable has a separate policy regarding acceptable use of the company's IT systems and all staff should ensure that they read and understand that policy as well as this social media policy.

This policy applies to the use of social media for both Enable and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using the organisation IT facilities and equipment or equipment belonging to members of staff.

Social Media Policy:

The purpose of this policy is to encourage good practice, to protect the organisation, its staff, clients and students; to clarify where and how existing policies and procedures apply to social media and to promote effective and innovative use of social media as part of the company's activities.

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 the company's equipment or facilities are used for the purpose of committing the breach.

Any member of staff suspected of committing a breach of this policy will be required to co-operate with the company's investigation, which may involve handing over relevant passwords and login details. Enable reserves the right to suspend internet access where it deems it necessary during an investigation.

When considering any potential breach of this policy, the organisation will consider the context of any social media posting.

Staff 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 result in disciplinary action.

Responsibilities:

The responsibility for drafting, updating, monitoring and reviewing this policy belongs to the (Health and Safety Officer) and it will be reviewed at appropriate intervals.

All employees are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to Senior Management.

If you have any concerns about information or conduct on social media sites that are inappropriate, offensive, demeaning or could be seen to be bullying, please report this to your line manager.

The IT Department is responsible for maintaining Enables computer systems and for supporting employees in the proper usage of the systems.

Safeguarding:

- Taking a lead role in investigating any reported incidents.
- Provide updates on best practice and highlighted Social Media platforms of concern.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.

E-Safety Group:

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy.
- Approve account creation o Receive completed applications for Social Media accounts.

Marketing and Curriculum leader:

- Create the social media account following approval.
- Store social media account details, including saving passwords securely.
- Be involved in monitoring and contributing to the account.
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring).

Staff:

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
- Attending appropriate training.
- Regularly monitoring, updating and managing social media accounts.

Social Media:

This policy is intended to ensure that staff understand the rules governing their use of social media in relation to their work for us, or when referencing Enable which may affect us or our activities. It is designed to help you use these platforms and services responsibly, to minimise the risks set out above and to ensure consistent standards of use of social media.

This policy therefore applies where:

• your use of social media relates to Enable or its activities

 • your use of social media relates to or is otherwise connected with your work, whether the intended use is personal or professional.

 • you represent yourself, or are otherwise identifiable, as someone employed by, or otherwise associated with Enable and its clients.

Appropriate Conduct:

You must not use your work email address to sign up for personal social media websites. When you create or exchange content using social media you are making a public statement.

 As such, your content will not be private and can be forwarded to third parties without your consent. You should therefore consider the potential sensitivity of disclosing information to the world.

Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it cannot be recovered, and this may result in liability for both Enable and yourself.

Take into consideration that, even if you are using social media in a personal capacity, other users who are aware of your association with us might reasonably think that you speak on the company's behalf.

When creating or exchanging content on a social media platform, you must always comply with your contract of employment (or other contractual relationship) with us, our disciplinary rules and any of our policies that may be relevant.

You must:

- not harass or bully other members of staff OR breach our harassment and bullying policy
- not promote political or social groups which are not aligned to Enable.
- not discriminate against other members of staff, students or third parties OR breach our equality policy.
- not breach our data protection, internet, email and communications, information security and/or whistleblowing policies.
- respect any confidentiality obligations owed by you or us, and not disclose commercially sensitive material or infringe any intellectual property or privacy rights of the College or any third party.
- not make defamatory or disparaging statements about Enable, its staff or students or organisation connected to the company.
- not create or exchange or link to abusive, obscene, discriminatory, derogatory, defamatory or pornographic content.

Relevant Policies and Procedures:

- Safeguarding Policy (2019
- Staff Disciplinary Policy
- Acceptable Use of IT
- Whistleblowing

Covid-19 Statement:

In the light of the Covid-19 Pandemic, we as an organisation has adapted our Digital Media Policy to follow the new Government Guidelines on how we us it to deliver our services to our students and sub-contractors.

To combat the spread of the Covid-19, between employees in the office, learners and sub-contractors who normally meet on a face-to-face basis, we have limited this contact and are working remotely from home and connect through various digital platforms which can have an impact on our online security.

A review all Covid-19 policy statements will be updated as and when Government guidance changes.