Social Media Policy and Procedure

The growth in social media, particularly Social media sites, has created increased opportunity for media communications that have an impact upon the College. The term 'social media' is used here to describe dynamic and socially-interactive, networked information and communication technologies, for example Web 2.0 sites, SMS text messaging and Social media sites.

While the College has clear guidelines and policies regarding other aspects of its operation, eg human resources, IT and corporate identity, these do not explicitly cover the usage of social media.

The purpose of these social media guidelines is as follows:

- to encourage **good practice**
- **to protect** the College, its staff and students
- to clarify where and how **existing policies** and guidelines apply to social media
- to **promote effective and innovative use** of social media as part of the College's activities.

In particular any official College Social media site / group must be approved by the College's Principal or Director. A central record will be kept of all approved sites (whether created by students, alumni, ETC staff members or the marketing department for official marketing purposes. All approved sites must have a designated administrator who is responsible for the content of the site.

General guidelines

- All current ETC International College policies concerning staff and students also apply to the use of social media. These include HR policies, codes of conduct, acceptable use of IT (see the Company Handbook) and disciplinary procedures. The following policy is of particular importance:
  ETC Safeguarding Policy and Procedures (Policy for the Protection of Juniors and Vulnerable Adults).
- Departments contacting alumni must consult the Marketing office first.
- Staff and students should take effective precautions when utilising Social media sites to ensure their own personal safety and to protect against identity theft.
- Staff and students need to consider intellectual property rights, copyright and ownership of data when using social media.
- The College supports staff using social media where it adds value to existing services; social media should not, however, be used where existing services offer equivalent functionality.
- Where staff use social media for personal purposes at work this should be done in line with the College's current IT guidelines and any local management guidance.
- Individuals should exercise caution when interacting with, and responding to, potentially contentious posts on social media sites.
- The College will continually review the use of social media and may modify its policies should the status of particular social media sites change, eg if charges are introduced, changes made to the way content is used, terms of use are changed, or if a site closes down.

Encouraged practice

- **Academic uses** – the College recognises that social media has the potential to support/advance learning opportunities and encourages its use in this way; social media should not, however, be used where existing learning resources or methodologies offer equivalent functionality.
- **Collaborative uses** – the College supports both internal (eg inter-department) and external (eg inter-College) collaboration and recognises that social media may provide opportunities for people and organisations to work together.

- **Communications and External Relations uses** – the College recognises the opportunity to communicate with prospective and existing customers through social media as part of an integrated marketing strategy.
- **Prospective and current students' uses** - these users, along with others who have an interest in the College, are active in social media, eg setting up Facebook groups and blogging. The Marketing department will monitor these sites to get further insight into the needs of its customers. Possible responses to any contentious issues identified in unofficial social media sites should be referred to the Principal or the Director.
- **Alumni uses** – the College recognises the opportunity to communicate with existing students and alumni through social media to develop an on-going relationship with them. These uses are the responsibility of the Marketing department, which has ultimate responsibility for Alumni contact details and will work closely with the Principal and the Director.
- **Sports and Social Activities department** – the College understands that the Sports and Social Activities department may want to use social media to maximise the exposure of its services to existing and prospective students. These uses are the responsibility of the Sports and Social Activities department.

Other potential uses

- The College will not refer to Social media sites when assessing student applications and job applications unless such sites are specifically highlighted in the application. The College will assess all applications only on the information provided.
- The College may refer to Social media sites when investigating breaches of discipline, eg cheating, harassment, anti-social behaviour. Further information on student disciplinary procedures can be found on the ETC website.
- The College may monitor forums and blogs to gain indirect feedback on College services and facilities. The College may post replies on forums or blogs to answer queries or address factual corrections, but would generally take a cautious approach before getting involved in contentious issues.
- The College reserves the right to take any necessary steps to protect its facilities, staff and students from malware (malicious software) including blocking sites where this is an issue.

IPR, copyright and ownership of data

Protecting IPR in your work

When you post content on a social media site, you should always make sure that you protect rights in the work that belong to you and / or the College. Check the site's terms and conditions to make sure it does not claim copyright to content posted, and that it does not state that any posted content becomes public domain.

A site's terms and conditions will usually state that by posting content you are giving consent for that site to publish that content. This consent should be non-exclusive (ie you are allowed to use the content elsewhere); all other rights and ownership should remain with you (ie you are only giving them the right to publish your content on their site, nothing more); you should be able to remove your content and when you do so this should end the site's rights (unless you've shared the content in a way that means it will persist on other users' profiles, etc); and you should be able to control access to your posted content through privacy settings or some other means, unless the site is entirely public and you are happy with that.

You should also consider how posting content on a social media site might affect other potential uses. For instance, posting a draft of a research paper or a book might damage your chances of finding a print publisher for that content if they consider the online posting to be prior publication.

IPR in the work of others

There are many misconceptions about how copyright law applies to the internet. Issues surrounding copyright and other intellectual property rights are rarely simple. As far as copyright is concerned, the rule of thumb should be to only ever use content (text, images, audio, video, etc) where you have explicit permission to do so. You should never, for example, use an image found through Google Images on a Facebook page.

It can be allowable to quote short extracts from another source if it's done for review or comment. Generally, though, if you wish to use content from another source you need to confirm that you are allowed to do so: if the content comes from another website that site may contain guidance setting out conditions for re-use; otherwise you may need to contact the rights-owner directly.

The informal nature of social media can encourage a relaxed attitude to rights issues, but you need to remember that the laws regarding copyright and intellectual property rights still apply.

Social Media uses on behalf of the College - Dos and Don'ts

If you have been charged with handling social media communications on behalf of ETC International College (ie. as part of ETC's wider marketing and PR operations, within the ETC marketing department), please use the following as a guide:

DO:

1- Engage in conversation
Interacting with an audience through various social media channels can be the fun part of building a brand online! Regularly contributing to relevant conversations is key to creating a strong dialogue with stakeholders.

2- Ensure a brand is consistent across networks and platforms
If practitioners confuse their audience, they will lose their audience. Ensure various social media profiles give off a similar 'vibe'. Keeping the style and tone of voice consistent will help an audience identify and engage with a brand.

3- Disclose relationships when endorsing an organisation/ client / customer
For example, if a practitioner tweets (or re-tweets) client news, it is best to include [client] at the end of the tweet. If a practitioner tweets (or re-tweets) its employers news on a regular basis, it is best they declare their relationship by including the name of their employer in biography section of the Twitter profile.

4- Be honest about who 'manages' social media channels
An individual: if a practitioner is updating a Twitter account, Facebook fan page or a YouTube channel on behalf of another individual, for example, a fellow employee or a client CEO, it is best to be open and clearly state '@person' typically 'manages' the channel. Preferably, this information should be outlined in the biography or administration sections of the social media platforms. For an organisation: if a practitioner is updating a Twitter account, Facebook fan page or a YouTube channel on behalf of an organisation or movement, then it can be assumed that the person or people managing the channel have a vested interest in the organisation. It is preferable to declare who 'manages' the channel but not necessary.

5- Outline content approval process from the offset
Work with the parties involved in social media activities to agree the process of approval at the beginning of the campaign. For example, each blog entry that has been ghost written must be approved by 'x', 'y' and 'z' executives. In addition, 'a' has permission to update Twitter account / Facebook page / YouTube channel on a regular basis and individual tweets / status updates / comments do not need to be approved.

6- Be transparent when updating information

If a practitioner is working with a community to update company or client related information it is important they are upfront about who they are and their intentions.
For example, if a practitioner is looking to update a Wikipedia entry on behalf of a company or a client, it is best visit the discussion / talk pages and work with an editor to update the relevant page – all updates and entries to Wikipedia must be neutral in tone, factual and verifiable. Please read the Wikipedia guidelines carefully before submitting or editing an article.

7- Correct errors openly and in a timely manner
Always admit errors and openly 'put them right'. It is advisable to tackle an online crisis as soon as possible to stop it escalating out of control.

8- Add a 'views are my own' disclaimer where appropriate
This disclaimer is typically needed if a practitioner uses an individual social media account to share both personal and professional opinion on matters. For example, it is advisable to add a 'views are my own' disclaimer to a Twitter biography, if a practitioner tweets about client and industry related news / opinions, [professional] and also shares their personal views on a subject that lies outside of their work remit [personal] through the same Twitter account. This will avoid confusion and will reinforce that a practitioner's personal opinion on issues is NOT the opinion of their company.

9- Be upfront about conflicts of interest and paid for opportunities
If writing or contributing to a blog which recommends a service supplier, make extra effort to make readers aware of any conflicts of interest, such as a financial or a partnership link between the client / member and the supplier.

10- Be respectful
Always seek permission when updating information and uploading images and videos featuring colleagues or clients to various social media platforms including but not exclusive to, Twitter, Facebook and YouTube.

DON'T:

1- Forget that a social media presence becomes part of a brand legacy
Posts, pictures, images, tweets, status updates (content in general) can stay online forever. Think about what message to share via social media channels.

2- Make an audience feel uncomfortable
It is good to be authentic and provide a hint of personality but continuously being grumpy or openly criticising people can put an audience off and deter them from engaging with an individual or organisation.

3- Bring a company into disrepute
It is likely that most legally binding contracts include a clause about employees not bringing an organisation into disrepute. It is important to remember this clause relates to online activity as well as offline activity. Refer to social media guidelines to understand the online boundaries at a specific organisation.

4- Reveal company / client sensitive information or intellectual property
Offline information that should be kept confidential such as new business wins should not be disclosed online unless specific permission has been granted by the parties concerned; or unless it is in the public interest; or unless required to do so by law.

ETC International College

Personal Use of Social Media Sites – Policy and Procedure

Purpose

The primary purpose of the Personal Use of Social Media Sites Policy and Procedure is to clarify for employees how they should conduct themselves when using all forms of social media sites. If followed, it will help employees to minimise the risk they may unintentionally place themselves and students in when they choose to write about their work. This in turn will avoid situations where safeguarding concerns could arise, employees' integrity could be undermined, the College or associated organisations be brought into disrepute and professional relationships with colleagues and students compromised.

Additionally, adhering to the policy reduces the risk of employees inadvertently contravening sections of the Data Protection Act or falling foul of libel, defamation and copyright laws.

Scope

The policy is appropriate to all staff members employed by ETC International College.

This policy is concerned with the personal use of social media sites, not with work / official social media sites. Employees wanting to create a work-related social media site must discuss this with and obtain approval from the Director / Principal. Ordinarily, this will only be authorised if the employee works within the ETC Marketing department.

This policy should be read in conjunction with the College's Company Handbook.

Principles

- The College's commitment to equality of opportunity will be observed at all times during the operation of this procedure. This will ensure that employees are treated fairly and without discrimination on the grounds of race, nationality, ethnic or national origins, gender, marital status, disability, age, sexual orientation, trade union membership or activity, political or religious belief and unrelated criminal conviction.

- This policy is not intended to prevent employees from using social media sites, but to make them aware of the risks they could face when sharing information about their professional and / or personal life.

- Employees should be encouraged to report any concerns that they have regarding content placed by employees on social media sites. Employees should report their concerns to their Line Manager / the Principal.

Roles and Responsibilities

Line Managers	Line Managers should ensure that all employees are aware of the Personal Use of Social Media Sites Policy and Procedure and of their responsibilities under it. It is the responsibility of the Line Manager to ensure that breaches of the policy are investigated and addressed – this may include referral to the Local Authority's Safeguarding Unit.
Employees	Employees are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place children or vulnerable adults at risk, bring the College into disrepute or damage their own professional reputation.

Procedure

Social media sites covered

This procedure covers the use of all types of social media sites, which include but are not limited to:

- Social networking sites e.g. Facebook, MySpace and Bebo
- Blogging
- Micro blogging sites e.g. Twitter
- Video Clips and Podcasts e.g. You Tube
- Discussion forums.

Responsibilities of employees

- Employees are personally responsible for the content they publish on social media sites. Employees must be mindful that what is published will be public for a long time.

- To avoid any conflict of interest, employees should not request or accept students under the age of 18 or vulnerable adults (eg. individuals with learning difficulties or disabilities) as "friends".

- Information must not be posted that would disclose the identity of students.

- Students must not be discussed on social media sites.

- Photographs or videos of students or their homes must not be posted on social media sites.

- Employees should not post information on sites, e.g. photographs and videos, that could bring the College or associated organisations into disrepute.

- Employees must not represent their own views / opinions as being those of the College or associated organisations.

- Potentially defamatory remarks towards the College, associated organisations, employees, students, students' relatives, suppliers and partner organisations should not be posted on social media sites.

- Employees must not either endorse or criticise service providers used by the College or associated organisations or develop on-line relationships which create a conflict of interest.

- Employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive or discriminatory language on social media sites.

- Employees must not divulge any information that is confidential to the College, associated companies or a partner organisation.

Security

Employees should be mindful when placing information on social media sites that it is potentially visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for false allegations and threats. In addition it may be possible through social media sites for children or vulnerable adults to be identified, which could have implications for their security.

Furthermore there is the scope for causing offence or unintentionally causing embarrassment, for example if students find photographs of their teacher which may cause embarrassment and / or damage to their professional reputation and that of the College. In addition, it may be possible for

other social media site users to identity where employees live, which could have implications for individual security.

Therefore, first and foremost consideration should be given to the information posted on social media sites and employees are advised to use appropriately the security settings on such sites in order to assist in limiting the concerns above (see Appendix).

Employee groups / networks

Employee groups can be created on social media sites such as Facebook. Creators of these groups are responsible for monitoring the content of the site and ensuring that it is appropriate.

Disciplinary action

Employees should be aware that the use of social media sites in a manner contrary to this policy may result in disciplinary action.

Employees using social media sites must not access social media sites for personal reasons during working time.

Any instances of “cyber bullying” will be addressed through the regular ETC Disciplinary Policy and may result in disciplinary action.

Appendix

Employee guidelines

1. Introduction

At the time of writing, there are over 250 million Facebook users around the world, making it the most popular social networking site. However, the use of social media sites like Facebook carries a great deal of risk. For example, Facebook profiles can often contain names, addresses and dates of birth. This can lead to anyone being able to set up a credit card in your name. Also, identity thieves would find it easier to piece together information about you from different websites / resources and use it to their advantage. This sounds unlikely but it is a real risk: the Press often carries stories about people who have lost money or had their credit rating damaged, which can be very tedious to correct.

Many employees are registered onto Facebook or similar websites such as Twitter, Bebo and MySpace. This guidance has been produced to help you, as an employee, ensure that correct privacy settings have been enabled within your Facebook profile. For other social networking sites, the same rules and risks apply in principle, so you are advised to become aware of what privacy settings are built into the site and take time to change the default settings.

2. Scope

This guidance document relates to all social networking websites including, but not limited to, Facebook, Bebo, Twitter and MySpace.

This document is not intended to encourage the use of Facebook or similar social networking sites, but rather to ensure that employees who use these websites are doing so safely.

3. Risks

There are many risks with using Facebook. Here are some risks that you need to be aware of:

- Anyone could find out information about you through the use of Facebook.
- Threatening messages could easily be sent through the use of Facebook.

- There are risks to professionalism and independence when working with children and vulnerable service users.
- Information posted within the status field could possibly tell everyone that you are on holiday and your house will be empty for a couple of weeks.
- There are potential risks to children who update their status to show their whereabouts.
- Damage can be done to the College's or associated organisations' reputation by posting inappropriate comments on another user's profile, which could be visible to everyone.
- Inappropriate photographs or offensive jokes can be posted on an employee's profile.

4. Facebook Privacy Overview

Facebook security is divided into separate parts: (see figure 1)

- **Account Settings** – To controls username / password details and to control what information you share with others.
- **Privacy Settings** - Security settings within the website to control what information is visible on your profile e.g. basic information, personal information, photos, wall posts and searching.
- **Application Settings** - Security in relation to the functionality of applications e.g. events, groups, videos and gifts.

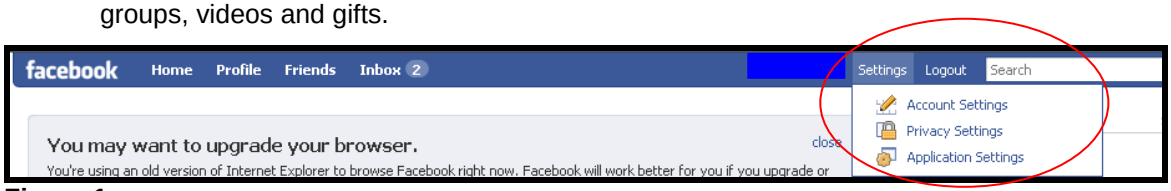

Figure 1

5. Account Setting Recommendations

5.1 Information entered into your profile and accepting friends' requests

If you have entered your date of birth within your profile, change the privacy settings to display just the day and not the year.

Do not mention your mother's maiden name, your favourite pet or your school history in your profile. These are the security questions web sites such as banks use as part of checking who you are or in their "forgot password" functions. Although we recommend that you don't, some people use their pet's name or mother's maiden name as passwords. By making this information available on your profile you may potentially be making it easier for people to hack your account.

If entering information or photos onto your profile, always bear in mind that a present or future employer could be viewing your profile.

Facebook provides every user with their own message board, also known as their "wall". The messages sent or received on your wall are displayed on your profile. Be careful about what is written on your wall and on your current status field, because others will be able to view the exchange of messages between you and your contact unless you secure your privacy settings (see Section 6 below for more information about privacy settings).

Examples of messages on user's wall which can be seen as a risk include:

- Telling your friends that you are going on holiday with the whole family – burglars would know there is an empty house and possibly your return date.
- Inviting your friends to a house party – this could lead to strangers inviting themselves along – this happened on a MySpace profile where a group of strangers turned up and caused thousands of pounds worth of damage to someone's house.

5.2 Accepting friend requests

Facebook encourages us to be friends with as many people as possible. Therefore some people may have a tendency to accept any friend requests they receive. As a Facebook user, you are advised to consider the following before accepting a friend request:

- Think carefully about who you allow as a friend
- Remember people may not be who they say they are
- If in doubt of a person's identity, do not accept the request.

6. Security / privacy settings within the website

Facebook offers a wide range of privacy settings to control who you share your information with, but it is up to you to ensure that these controls are set at an appropriate level. It is important to explore all the options under the privacy heading and amend the ones you feel are relevant. When using any social networking website, never use the standard default privacy settings, as these are more likely to leave your account open for other users to view.

This section gives you further details of the main privacy settings available on Facebook and how they can help you control the way you share your information. Make time to view them all and decide on what level you wish to set them at.

6.1 Profile

By default, Facebook allows all your friends and networks (e.g. groups) to view your profile information. Networks can contain many thousands of people so you will be leaving your information visible to these users if you keep this on the default setting.

Facebook allows users to secure your profile using the privacy settings. There are three settings to choose from.

- **Making your profile available to everyone**
  This will make your profile available to everyone and anyone. This is not recommended.

- **Making your profile available to your friends and networks**
  This setting allows all your friends and networks to view your profile. Friends are usually the contacts that you have created/received a request from and will only appear on your contacts list when both users have clicked "accept".

  Your profile would be open to anyone else within your network, i.e. all the groups / networks that you have joined. Again this opens your profile to anyone else that is listed as a member.

- **Making your profile available to your friends only**
  This is the most secure option and is recommended. Other people can still search for you, but they would not be able to view your profile / photographs or comments until they are listed as a friend in your contacts list.

6.2 Search

You are able to change a setting within the privacy tab to stop people from finding your profile when they perform a search. The Facebook search facility makes it easy for anyone to enter your first name and / or surname into the search field and find a list of all the users on the site matching that name. Users are then able to sort within the results to narrow down the list of names more specifically by using other sorting options e.g. by locations, age, status, gender, location and many more.

The following settings can be changed in relation to searching:

Allow anyone to see my public search listing
If you want people you know to know that you are on Facebook, leave this unselected.

Allow my public search listing to be indexed by external search engine

If set to “yes”, your details will be available via search engines such as Google and MSN.

If you allow others to search for your profile within Facebook, they will be able to do the following:

- See your profile pictures
- Send you a message
- Add you as a friend
- View your friend list
- If you haven’t restricted your profile settings (see Section 5.1 above), the person who performed the search can view your profile fully.

6.3 Poke Messages and Friend Requests

Sending a poke, replying to a message or receiving a friend request temporarily allows that user to view your profile even if your normal privacy settings would not allow them to do so. This area allows you to control what profile information you wished to be visible. You should also be careful about whom you reply to. If in any doubt, you could block a user.

6.4 Block People

An option is available to block another user. They will not be able to search for you, view your profile or contact you on Facebook. Any current connections you have with that user will be removed (e.g. friendship, relationship). You can use this if you are having problems with a particular person trying to contact you.

7. Application Settings

Applications within Facebook include additional “add on” functionality, so for example, interest groups, games, events, videos, etc.

You can edit the settings to allow or restrict the view of which applications you have added to your profile. You can customise this to allow selected friends to see which applications you have added but not all. The following options are available to choose from:

- Everyone
- My network and friends
- Friends of friends
- Only friends
- Only me
- Customise.

This version:
Author: David Jones.
Date: 3rd October, 2018.