Social Media Policy

Business Area: **Human Resources**

Version: **1.2**

Document Ref: **POL-15-057**

Document Control

Status: LIVE

Document Version History

Date	Version	Author	Comments
26/04/18	0.1	[redacted]	First Draft
27/04/18	0.2	[redacted]	Minor edits to document
12/05/17	0.3	[redacted]	RACI Model added prior to publish for first review on DCS
07/06/17	1.0	[redacted]	Added policy update strap line, moved to live after consultation with PCS Union
11/05/18	1.1	[redacted]	Completed annual review
11/05/18	1.2	[redacted]	Re-templated and annual review complete Burness Paull comments incorporated into document

Review and Approval Register

Note: RACI = R- Responsible, A- Accountable, C-Consulted, I-Informed

Name	Position	RACI Role
[redacted]	Head of Assurance Services/ Company SecretarySIRO/DPO	I
[redacted]	Information Assurance Accreditor/Deputy DPO	I
[redacted]	Information Governance & Compliance Manager/Deputy SIRO	C
Adrian Tucker	Chief Information Officer (Interim)	I
[redacted]	Chief Information Technology Security Officer	C
[redacted]	Chief Technical Officer	I
[redacted]	Hr Business Manager	R
Bernice McNaught	HR Director	A
PCS	SLC Union	I
[redacted]	Social Media Manager	C
[redacted]	Social Media Manager	C

Update Schedule

This document will be reviewed at least annually or whenever business requirements, legislation, regulations change.

Applicability

The requirements in this document apply to:

- All permanent, temporary and contract workers employed or engaged by SLC or any 3rd party organisations whilst at work or engaged on SLC business.

Compliance

- *Any employee found to have violated these requirements could be subject to disciplinary action, up to and including termination of employment.
- *At its sole discretion, SLC may require the removal from the service provision account any employee of a 3rd party organisation contractually engaged on SLC business who is found to have violated these Procedure requirements.

* Amend/Delete as appropriate>

Contents

1.1 Statement

Employees of the Student Loans Company Limited (SLC) may be able to access social media services and social networking sites at work, either through company IT systems or via their own personal equipment.

This Social Media Policy describes the rules governing use of social media within SLC. It sets out how staff must behave when using the company's social media accounts or discussing SLC on their personal account.

This policy should be read alongside other key policies. The company's internet use, data protection and acceptable use policies are particularly relevant to staff using social media

1.2 Purpose

Social media can bring significant benefits to SLC particularly for building relationships with current and potential customers; however it is important that employees who use social media do so in a way that enhances the company's profile.

A misjudged or incorrectly posted status update can generate complaints or damage the company's reputation; there are also security and data protection issues that must be taken in to account.

2 Scope

Regardless of which social network employees are using, or whether they are using business or personal media accounts on business time, following these rules will help to avoid the most common pitfalls:

- **Know the social network –** Employees should spend time becoming familiar with the social network before contributing. It is important to read any FAQs and understand what is not acceptable on a network before posting.
- **If unsure, don't post it –** Staff should always err on the side of caution when posting to social networks. If an employee feels an update or message might cause offence - or be unsuitable they should not post it and seek advice from the Corporate Communications Team.
- **Be thoughtful and polite –** Many social media users have got into trouble simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used when communicating by email.
- **Look out for security threats –** Staff members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware.
- **Handle complex queries via other channels –** Social networks are not a good place to resolve complicated enquiries and customer issues. Once a customer has made contact, employees should handle further communication via the most appropriate channel – usually email or telephone.

- **Don't escalate things -** It is easy to post a quick response to a contentious status update; employees should always take time to think before responding, and hold back if they are in any doubt.

2.1 Use of Company Social Media Accounts

2.1.1 Authorised Users

Only people who have been authorised to use the company's social networking accounts may do so.

Authorisation would normally be authorised by the SLC Social Media Manager. It is normally granted when social media tasks form a core part of the role of the employee.
Allowing only designated people to the use these accounts ensures the company's social media presence is consistent and cohesive.

2.1.2 Creating Social Media Accounts

New social media accounts must not be created in the company's name unless authorised by the SLC Social Media Manager.

The company operates its social media policy presence in line with a strategy that focuses on the most appropriate social networks, given available resource.

2.1.3 Purpose of Company Social Media Accounts

In general, employees should only post updates, messages or otherwise use these accounts when that use is clearly in line with the company's objectives.

For instance, employees may use social media accounts to:

- Respond to **customer enquiries** and requests for help
- Share **blog posts, articles and other content** created by the company
- Share **insightful articles, videos media and other content** relevant to the business, but created by others
- Provide followers with **an insight into what happens within the company**
- Support **new product launches** and other initiatives
- Publish government announcements

2.1.4 Inappropriate Content and Uses

Company social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the company into disrepute.

When sharing an interesting blog, post, article or piece of content, employees should always review the content thoroughly, and should not post the link based solely on a headline.

2.1.5 The Value of Social Media

SLC recognise that employees' social media accounts can generate a number of benefits, for instance:

- Staff members can make **industry contacts** that may be useful in their jobs
- Employees can discover content to help them **learn and develop** in their role
- By posting about the company, staff members can help to **build a positive business profile** online

2.1.6 Safe Responsible Social Media Use

The rules in this section apply to:

- Any employee using company social media accounts
- Employees using social media accounts during company time

Users must not:

- Create or transmit material that might be **defamatory or incur liability** for the company.
- Post messages, status updates or links to material or content that is inappropriate.
  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling or illegal drugs.

  This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political belief, national origin, disability, sexual orientation or any other characteristic protected by law.
- Use social media for any **illegal or criminal activities.**
- Send **offensive or harassing material** to others via social media.
- Broadcast **unsolicited views** on social, political, religious or other non-business related matters.
- Send or post messages or material that **could damage SLC's image or reputation.**
- Discuss **colleagues, customers or suppliers** without their approval.
- Post, upload, forward or link **spam, junk email, chain emails and messages.**

2.1.7 Copyright

SLC respects and operates within the copyright laws;, users may not use social media to:

- Publish or share **copyrighted software, media or materials owned by third parties,** unless permitted by that third party
- If staff wish to **share any content published on another website**, they are free to do so if that website has obvious sharing buttons or functions on it
- Share links to **illegal copies** of music, films, games and other software

3.1 Security and Data Protection

Employees should be aware of the security and data protection issues that can arise from using social networks. Personal information processed by employees must be processed in accordance with SLC's Data Protection Policy.

3.1.1 Maintain Confidentiality

Users must not:

- Share a link to any content or information owned by the company that could be considered **confidential or commercially sensitive.**
  - This may include details of key suppliers or information relating to any future strategy within SLC.
- Share a link to any content or information owned by another company or person that could be considered confidential or commercially sensitive
- Share a link to personal information that could breach SLC’s Data Protection Policy

3.1.2 Protect Social Accounts

- SLC social media accounts should be **protected by strong passwords** that are changed at regular intervals and shared only with authorised users
- Wherever possible, employees should use **two-factor authentication** to safeguard company accounts
- Staff must not use a new piece of **software, application or service** without first seeking guidance from ICT security and approval from the SLC Social Media Manager.

3.1.3 Avoid social scams

- Staff should watch for **phishing attempts**, where scammers may attempt to use deception to obtain information relating to either SLC its suppliers or its staff

  Employees must never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information can be shared.

- Employees should **avoid clicking links** within posts, updates and direct messages that look suspicious. In particular, users should look out for URL's contained in generic or unexpected direct messages.

4.1 Monitoring Social Media

SLC IT and internet resources – including computers, smart phones and internet connections are provided for legitimate business use.

SLC therefore reserves the right to monitor how social networks are used and accessed through these resources.

Any such monitoring or examination will only be carried out by authorised staff.

All data relating to social networks written, sent or received through SLC systems is part of official company records.

The company can be legally compelled to show information to law enforcement agencies or other parties.

4.2 Related Documents

This Procedure forms an essential part of SLC's overall Information Risk Management arrangements and should be read in association with relevant related Procedure and supporting procedures, including:

Document Description
Acceptable Use Policy
Systems Access Control Policy
Data Protection Policy