Social Media Policy

January 2023

1. Introduction

IPS★ITCS★ITCS recognizes that the Internet provides a unique opportunity to participate in interactive discussions and share information using a wide variety of social media, such as Facebook, Twitter, and blogs. Employees are likely to use social media in a private capacity outside of work and they may also be required to use it in a business capacity as part of their role at IPS★ITCS.

However, employees' use of social media in both a personal and business capacity can present risks to our confidential information and reputation and can jeopardise our compliance with legal obligations. To minimise these risks, and to ensure that our IT resources and communications systems are used appropriately, we expect employees to adhere to this policy.

The purpose of this policy is to assist employees by providing clear guidance about acceptable behaviour on social media both at work and out of work. It is consistent with the regulations and conditions of service employees should already be aware of in their work for IPS★ITCS.

2. Scope

This policy applies to all employees of IPS★ITCS.

The policy also applies to contractors, agency workers, volunteers and those on apprenticeships and student/work experience placements, working on behalf of IPS★ITCS.

This policy applies to the use of social media for both business and personal purposes, whether during office hours or otherwise. It also applies whether the social media is accessed using IPS★ITCS facilities, or equipment belonging to members of staff.

This policy should be read in conjunction with the Employee Code of Conduct, Harassment and Bullying Procedure, and Internet and Email Acceptable Use procedure.

3. Exclusions

The social media policy will not apply where there are other separate, specific IPS★ITCS procedures to address an issue.

4. Definitions

Social media is a type of interactive online media that allows parties to communicate instantly with each other, or to share data in a public forum. This includes online social forums such as Instagram, Medium, Twitter, Facebook, LinkedIn, internet newsgroups,

and chat rooms. Social media also covers blogs, video and image sharing websites such as YouTube and Flickr.

There are many more examples of social media than can be listed here and this is a constantly changing area. This policy refers to the examples listed, and any new social media which is developed in the future.

5. Personal Safety and Privacy

Employees need to be aware that the information they post on their personal social media profile can make them identifiable to service users, as well as people they know in a private capacity.

Employees should therefore consider this when setting up their online profile particularly in relation to; use of a photograph, providing details of their occupation, employer, and work location.

Employees should ensure that clients known to them through their work, *where there could be a conflict of interest*, are not linked to them through social media. IPS★ITCS considers it inappropriate to have service users as 'friends' through social media, especially where these people are vulnerable and there may be safeguarding issues.

Online sites such as Facebook are in the public domain, and personal profile details can be seen by anyone, even if users have their privacy settings on the highest level. Also if a user's profile is linked to other sites, any changes to their profile will be updated there too.
Employees who have set their privacy level to the maximum can have their privacy compromised by 'friends' who may not have set their security to the same standard.

6. Key Principles

6.1 Personal accountability and responsibility

All employees are expected to behave appropriately and responsibly and should be aware that they may be accountable to IPS★ITCS for actions outside of their work.

Online conduct is the employee's responsibility, and it is important that employees are aware that posting information on social networking sites in a personal capacity cannot be entirely isolated from their working life.

Any information published online can be accessed around the world within seconds and will be publicly available for all to see and is not easy to delete/withdraw once published.

IPS★ITCS views any comment that is made on a social media site is made publicly, and that any inappropriate comment made, will be considered in the context of which it is made.

For example, disparaging comments against a colleague made to all friends on Facebook could be viewed as bullying/harassment or could be considered to bring IPS★ITCS into disrepute.

Employees are advised to be mindful that all comments made through social media must meet the standards of the Data Protection Act, the Employee Code of Conduct and the Equality and Diversity policy.

Employees may be accountable for actions outside of work, including making comments on social media sites, if that is contrary to any of IPS★ITCS's policies, impacts on or compromises the employee's ability to undertake their role, or undermines management decisions. Such behavior could be investigated and may result in disciplinary action being taken, and ultimately could result in dismissal.

Further employee guidance is available in the Appendix.

6.2 Access to social media for work purposes

Staff who use social media as part of their job must adhere to IPS★ITCS's Media Policy. Employees must be aware that they are representing IPS★ITCS when they are contributing to IPS★ITCS's social media activities. Employees should use the same safeguards as they would with any other form of communication about the organization in the public domain.

6.3 Access to social media at work, for personal use

Employees are not allowed to access social media websites for personal use from IPS★ITCS's computers or devices during working time and they must not be left running 'in the background', while at work. These provisions also apply to personal computers and mobile devices.
Leaving Social Media sites 'running' constantly in work time is considered to be a breach of the acceptable use of the internet policy.

6.4 Any communications that employees make through social media must not:

- **Bring the organization into disrepute, for example by:**
  - Criticising, disagreeing, or arguing with customers, colleagues, or managers.
  - Making defamatory comments about individuals or other organizations/groups.
  - Posting images that are inappropriate or links to inappropriate content.

- **Breach confidentiality, for example by:**
  - Referring to confidential information about an individual (such as a colleague or service user) or IPS★ITCS

- **Do anything that could be considered discriminatory against, or bullying or harassment of, any individual or group of individuals, and in contravention of IPS★ITCS's procedures, for example by:**
  - Making offensive or derogatory comments relating to sex, gender -reassignment, race (including nationality), disability, sexual orientation, religion or belief or age.
  - Using social media to bully another individual (such as an employee of IPS★ITCS); or
  - Posting images that are discriminatory or offensive or links to such content.

- **Any other action that impacts on the employee's ability to do their job, for example by:**
  - Online activity that is incompatible with the position they hold in IPS★ITCS
  - Any breach occurring inside or outside the workplace that is likely to affect the employee doing his/her work.

- **Contravene IPS★ITCS's policies, for example.**
  - The Employee Code of Conduct, the Harassment and Bullying policy, or the Equality and Diversity policy.

The above examples are not a definitive list of the misuse of social media but are examples to illustrate what misuse may look like. Employees are encouraged to talk to their manager and seek advice if they are unclear.

7. Addressing allegations of misuse

All employees are required to adhere to this policy. Comments made through social media may constitute an act of misconduct or gross misconduct, which could lead to dismissal, if the comments contravene any of IPS★ITCS's policies or if they lead to a breakdown in the relationship of mutual trust and confidence.

Managers should ensure that all complaints are dealt with consistently and fairly.

8. Roles and responsibilities

Employees have a responsibility to:

- Avoid behaviour that may cause an individual to feel the subject of harassment or bullying.
- Familiarise themselves with the Social Media policy and employee guidelines to using social media in the Appendix.
- Act responsibly when using online media for work and personal use.
- Report instances to their manager if they are subject to abuse

Managers have a responsibility to:

- Familiarise themselves with the Social Media policy and employee guidelines to using social media in the Appendix.
- Take prompt action to stop any harassment or bullying they become aware of, whether a complaint has been raised or not
- Ensure staff are aware of the Social Media policy and employee guidelines
- Support employees who are the subject of abuse through existing practices
- Ensure all complaints/allegations are dealt with fairly and consistently, and in accordance with other employment policies where appropriate.

HR staff have a responsibility to:

- Provide support and advice to managers and employees on the operation of the policy and guidelines, where necessary.

9. Further Guidance

An Employees' Guide to the use of social media is attached in the Appendix.

This policy also works alongside other policies including the Internet and Email Acceptable Use Policy, Employee Code of Conduct, Disciplinary Procedure and the Harassment and Bullying Procedure, copies of which are available on DNET or from your manager.

APPENDIX

EMPLOYEE GUIDANCE ON THE USE OF SOCIAL MEDIA

- Employees must be mindful that any online activities/comments made in a public domain, must be compatible with their position within IPS★ITCS, and safeguard themselves in a professional capacity.
- Protect your own privacy. To ensure that your social network account does not compromise your professional position, ensure that your privacy settings are set correctly.
- Comments made outside work, within the arena of social media, do not remain private and so can have an effect on or have work-related implications. Therefore, comments made through social media, which you may intend to be “private” may still be in contravention of the Employee Code of Conduct, the Harassment and Bullying Policy and/or the Disciplinary Policy. Once something is online, it can be copied and redistributed making it easy to lose control of. Presume everything you post online will be permanent and can be shared.
- Do not discuss work-related issues online, including conversations about service users, complaints, management or disparaging remarks about colleagues or IPS★ITCS. Even when anonymized, these are likely to be inappropriate. In addition doing this in the presence of others may be deemed as bullying and/or harassment.
- Do not under any circumstances accept friend requests from a person you believe could be a service user or may conflict with your employment.
- Be aware that other users may access your profile and if they find the information and/or images it contains offensive, make a complaint about you to IPS★ITCS as your employer.
- Ensure that any comments and/or images cannot be deemed defamatory, libelous or in breach of copyright legislation.
- When setting up your profile online consider whether it is appropriate and prudent for you to include a photograph, or provide occupation, employer or work location details.
- You can take action if you find yourself the target of complaints or abuse on social networking sites. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others.
- If you do find inappropriate references and/or images of you posted by a ‘friend’ online you should contact them and the site to have the material removed.
- If you are very concerned about someone else's behaviour online, you should take steps to raise your concerns. If these are work related you should inform your manager.

- Employees should also act in accordance with IPS★ITCS's Employee Code of Conduct, Internet and Email Acceptable Use Policy, and Harassment and Bullying Procedure.
- Employees should not access social media sites or leave these running in the background during working time, *for personal use*, on any devices within their control.

Revision History

Rev	Rev Date	Rev By	Approved By	Description
1.0	1/3/2022	Shayne Torrans	Shayne Torrans	Initial Procedure
1.1	11/23/2022	Shayne Torrans	Shayne Torrans	Format Revision

Approvals:

Procedure Owner

_____ _____
Print Name Date

_____
Signature

Competency Assessment

No.	Questionnaire	C/NYC
Q1		
A1		
Q2		
A2		
Q3		
A3		
Q4		
A4		
Q5		
A5		

Enclosed Attachments	
Risk Assessment	☑
Environmental Aspect and Impact	☑
Training and Competency	☑
Measure and Evaluation Tools	☑

Competency Checklist

To be filled out by Trainer and signed by Employee, Assessor and Supervisor before being returned to the HSEQT Manager for recording purposes.

Procedure	Competency	Date	Competent YES / NO	Employee Signature

(Please tick appropriate box)

This employee is competent in performing the job. ☐

This employee has not attained the competency level. ☐ *

* *If the employee has not attained all competency levels, the General Manager must assess the action to be taken, provide an extension of training or alternative action as listed below.*

Alternate action to be taken: _____

Signed By

Employee: _____ Date: _____

Trainer: _____ Date: _____

Assessor: _____ Date: _____

Regional Manager: _____ Date: _____

Environmental Aspects and Impacts

Identified Environmental Aspects and Impacts

The following table is a summary of the likely environmental aspects and impacts that may be identified during site inspections. The significance of each impact needs to be assessed using the Risk Assessment Model.

Activity	Aspect	Impact
Purchasing & Administrative Work	Consumption of goods	Conservation of natural resources
	Consumption of energy (eg. Electrical equipment and facilities)	Release of greenhouse gases and atmospheric pollution; Consumption of natural resources; Habitat loss
	Generation of waste (eg. Paper)	Consumption of space for waste disposal; Habitat loss
Climate Control	Consumption of energy	Release of greenhouse gases and atmospheric pollution; Consumption of natural resources; Habitat loss
	Generation of noise	Disturbance to community; Habitat loss
Cleaning of – offices / vehicles	Storage, use and release of chemicals	Contamination of air, water or soil; Risk to human health
Transport (Fleet vehicles / staff travel)	Consumption of energy	Release of greenhouse gases and atmospheric pollution; Consumption of natural resources; Loss of habitat at all stages of generation; Light pollution
	Consumption of goods (eg. Oil)	Consumption of natural resources; Generation of waste; Habitat loss; Biodiversity impacts
	Generation of waste (eg. Oil)	Consumption of space for waste disposal; Potential contamination of water or soil; Habitat loss
	Exhaust emission	Release of greenhouse gases and atmospheric pollution
	Use of dangerous goods (eg. Batteries)	Potential contamination of air, water or soil; Risk to human health
	Generation of noise	Disturbance to community; Habitat degradation
Operations		

Risk Assessment

Risk Assessment // insert name here					
Step No: Logical sequence	**Sequence of Basic Job Steps documented in the Procedure, Work Instruction and project plans. Break down Job into steps.** Each step should be logical and accomplish a major task.	**Potential Safety & Environmental Hazards/Impacts at the site of the Job** Identify the actual and potential health and safety hazards and the environmental impacts associated with each step of the job.	**Risk Rating** Refer to the risk matrix or HSEQT.PRO. Risk Mgt	**Recommended Corrective Action or Procedure** ***Determine the corrective actions necessary to reduce the risk to as low as reasonably practical (ALARP) refer to HSEQ.PRO.Risk Mgt. The risk must be rediced or controlled to ALARP before work commences.*** Document who is responsible for implementing the controls to manage each hazard identified.	**Risk Rating** refer to the risk matrix or HSEQT.PRO.Risk Mgt
1.					
2.					
3.					
4.					
5.					

Audit

Process: insert// **Procedure**: Insert //	Date:	Audited by:
	Location of Audit:	Area Mgr/Supervisor:

Item	Question	Evidence Sited	Comments	Conformance Score 0,3,5
1.				
2.				
3.				
4.				
5.				
6.				
7.				

AUDITOR'S SIGNATURE: SAFETY REP'S SIGNATURE:	CONFORMANCE SCORE: / 25 CONFORMANCE %:	0 – Non-Conformance 3 – Continuous Improvement Opportunity 5 – Total Conformance