IT POLICY

SCCU LIMITED

VERSION 1.0

Contents

Version Control

VERSION	REVIEWER NAME	DATE	NEXT REVIEW	COMMENTS
1.0	Liam Morrissey & Cheryl Wiley	04/08/2023	August 2024	

Introduction

1. This Policy applies to all employees, contractors, and agents of SCCU.
2. Employees are encouraged to use email and the internet at work as a fast and reliable method of communication with significant advantages for business.
3. In light of the fact that communications made by Employees and their other activities online reflect upon the Company and are capable of creating a number of commercial, professional, and legal problems, this Policy is intended to clarify what the Company expects from Employees and their responsibilities when using the Company's communications, email, and internet facilities.
4. The Company's Internet and Communication Facilities include:
    - Telephone
    - Email
    - Internet
5. Whilst the Company's Internet and Communications Facilities are made available to Employees for the purposes of the business, a certain amount of limited personal use is permitted insofar as such personal use is consistent with this Policy and the duties of the Employee.
6. In addition to this Policy, when using the Company's Internet and Communications Facilities, Employees must also comply with other Company Policies including the Company's Data Protection Policy, Equality & Diversity Policy.

General Principles

7. There are certain general principles that should be borne in mind when using any type of communication, be it external or internal, including hard copy letters, memos, and notices. The Company expects all Employees to:
    - Use the Company's Internet and Communication Facilities, and non-electronic facilities including but not limited to Company letterheads and stationery, responsibly and professionally and at all times in accordance with their duties;
    - Be mindful of what constitutes confidential or restricted information and ensure that such information is never disseminated in the course of communications without express authority;
    - Be mindful of what constitutes personal data and ensure that personal data relating to learners, clients and employee's is never disseminated in the course of

communications unless it is used in accordance with the Company's Data Protection Policy and with express authority;

- Ensure that they do not breach any copyright or other intellectual property right when making communications;
- Ensure that they do not bind themselves or the Company to any agreement without express authority to do so; and
- Be mindful of the fact that any communication may be required to be relied upon in court, to the advantage or the detriment of the individual or the Company, and to conduct their use of communication systems and equipment accordingly.
- The viewing, transmission, downloading, uploading, or accessing in any way of any of the following material using the company's internet and communications facilities will amount to gross misconduct with the possibility of summary dismissal:
    - Material, which is pornographic, sexist, racist, homophobic, or any other discriminatory or otherwise offensive material;
    - Illegal or criminal material, including material which breaches copyright or any other intellectual property right;
    - Any material which has the object or effect of causing harassment to the recipient; or
    - Material which the Employee knows, or reasonably ought to know, is confidential or restricted information and which they are not authorised to deal with.

Internet Use

8. The Company provides access to the internet for the sole purpose of business and to assist employees in the performance of their duties. However, the Company recognises that employees may need to use the internet for personal purposes and such use is permitted provided it is reasonable and does not interfere with the performance of their duties. Employees may be asked to justify the amount of time they have spent on the internet or the sites they have visited.

9. Employees must not use the internet to gain or attempt to gain unauthorised access to computer material or private databases, including restricted areas of the Company's network. Nor must they intentionally or recklessly introduce any form of malware, spyware, virus, or other malicious software or code to the communications equipment or systems of the Company.

10. Employees must not access or attempt to access any information which they know or reasonably ought to know is confidential or restricted.

11. Employees must not access or use personal data online in any manner that is inconsistent with the Company's Data Protection Policy.

12. Employees must not download or install any software without the express permission of the Operations Manager.

13. Employees must not attempt to download, view, or otherwise retrieve illegal, pornographic, sexist, racist, offensive, or any other material which is in any way in bad taste or immoral. Employees should note that even material that is legal under UK law may nonetheless be in sufficiently bad taste to fall within this definition. As a general rule, if any person might be offended by any content, or if that material may be a source of embarrassment to the Company or otherwise tarnish the Company's image, viewing that material will constitute a breach of this Policy. Any such attempt will constitute a disciplinary offence and in addition to internet access being reviewed, reduced, or withdrawn, may be subject to disciplinary action or summary dismissal.

Social Media Use

14. Employees may use social media for personal purposes occasionally during work hours for example, during breaks, provided that such usage complies with the provisions of the Company's Social Media Policy and provided that it does not interfere with their work responsibilities or productivity.

15. The Company recognises that in their private lives Employees may wish to publish content on the internet through a variety of means, including social media. Even outside of work Employees must refrain from doing anything on social media or any other websites that defames, disparages, or otherwise brings into disrepute, the Company, an Employee's superiors, an Employee's colleagues, or other related third parties. This includes, but is not limited to, making false or misleading statements and impersonating colleagues or third parties.

16. If an Employee makes any posting, contribution, or creation or publishes any other content which identifies or could identify the Employee as an employee, contractor, agent, or other member or associate of the Company, or in which the Employee discusses their work or experiences relating to the Company, the Employee must at all times ensure that their conduct is appropriate and consistent with their contract of employment and the corporate image of the Company, and should bear in mind that the Employee owes a duty of fidelity to the Company.

17. If an Employee is unsure as to the appropriateness of a posting or other content they wish

to publish, they should speak to the Operations Manager at the earliest opportunity to seek clarification.

18. If, in any contribution or posting which identifies or could identify the Employee as an employee, agent, or other affiliate of the Company, the Employee expresses an idea or opinion, they should include a disclaimer which clearly states that the opinion or idea expressed is that of the Employee and does not represent that of the Company.

Company Email Use

19. The email address which employees are provided by the Company is provided for business purposes in order to facilitate information sharing and timely communication. Any Company business which is conducted via email must be conducted using Company email and is under no circumstances to be conducted through any other personal email address or account.

20. Employees should adopt the following points as part of best practice:

- Before communicating via email, Employees should satisfy themselves that it is the most suitable mode of communication, particularly where time is of the essence;
- Ensure that the email contains the Company disclaimer notice. This should be added automatically by the email client. If it is not, notify the Operations Manager immediately;
- All emails should contain the appropriate business reference(s), either in the subject line or in the body of the text;
- Emails should be worded appropriately and in the same professional manner as if they were a letter;
- Employees should be careful not to copy an email automatically to everyone copied into the original message to which they are responding as this may result in inappropriate or unlawful disclosure of confidential information and/or personal data;
- Employees should take care with the content of emails, in particular avoiding incorrect or improper statements and the unauthorised inclusion of confidential information or personal data. Failure to follow this point may lead to claims for discrimination, harassment, defamation, breach of contract, breach of confidentiality, or personal data breaches;

- All emails should be proofread before transmission, which includes ensuring that any attachments referred to in the text are actually attached and are correct and the intended recipients' email addresses are correct;
- If an important document is transmitted via email, the sender should telephone the recipient to confirm that the document has been received in full;
- Employees must not email any business document to their own or a colleague's personal and/or web-based email accounts.
- Employees may use Company email for personal purposes, provided that such use is kept to a minimum and does not interfere with the performance of the Employee's duties. In any case Employees are not permitted to use their Company email address to subscribe to any newsletters or to receive any marketing, as this will result in extra unnecessary burden being placed upon the Company's communications systems. All personal emails should be labelled "personal" in the subject line.
- If Employees do use Company email for personal reasons, they will be deemed to agree to the possibility that any emails sent or received may be subject to monitoring in accordance with this Policy.
- Employees must not send abusive, obscene, discriminatory, racist, harassing, derogatory, pornographic, or otherwise inappropriate material in emails. If any Employee feels that they have been or are being harassed or bullied, or if they are offended by material received in an email from another Employee, they should inform their line manager.
- Employees should at all times remember that email messages may have to be disclosed as evidence for any court proceedings or investigations by regulatory bodies and may therefore be prejudicial to both their and the Company's interests. Employees should remember that data which appears to have been deleted is often recoverable. If secure deletion is required, for example, where an email contains confidential information or personal data, Employees should follow the steps set out in the Company's Data Protection Policy.

Personal Email Use

21. Employees are permitted to access and use their personal email accounts only to the extent that such use is reasonable and does not interfere with the Employee's performance of their duties.

Company Telephone System Use

22. The Company's telephone lines and mobile phones issued by the Company are for the exclusive use by Employees working on the Company's business. Essential personal telephone calls regarding Employees' domestic arrangements are acceptable, but excessive use of the Company's telephone system and/or mobile phones for personal calls is prohibited. Acceptable use may be defined as no more than one personal call in a working day. Any personal telephone calls should be timed to cause minimal disruption to Employees' work.

23. Employees should be aware that telephone calls made and received on the Company's telephone lines, and mobile phones issued by the Company, may be routinely monitored to ensure customer satisfaction or to check the telephone system is not being abused.

24. If the Company discovers that the telephone system or a mobile phone issued by the Company has been used excessively for personal calls, this will be treated as a disciplinary matter and will be handled in accordance with the Company's disciplinary procedures.

Personal Mobile Phone Use

25. Essential personal telephone calls regarding Employees' domestic arrangements are acceptable, but excessive use of Employees' own mobile phones for personal communications (including, but not limited to, calls, messaging, emailing, and web browsing) is prohibited. In order to avoid disruption to others, mobile phones should be set to silent during normal working hours.

26. Any personal telephone calls on Employees' own mobile phones should be timed to cause minimal disruption to Employees' work and to colleagues working nearby.

Security

27. The integrity of the Company's business relies on the security of the Company's Internet and Communications Facilities. Employees bear the responsibility of preserving the security of Company's Internet and Communications Facilities through careful and cautious use. In addition to the general provisions contained in this Policy.

28. Access to certain websites and online services are blocked. Often the decision to block a website or service is based on potential security risks that the site or service poses. Employees must not attempt to circumvent any blocks placed on any website or service by the Company.

29. Employees must not download or install any software or program without the express permission of the Operations Manager.

30. Employees must not delete, destroy, or otherwise modify any part of systems (including, but not limited to, hardware and software) without the express permission of the Operations Manager.

31. Employees must not share any password with any person, other than when it is necessary for maintenance or repairs by IT support staff. Where it has been necessary to share a password, the Employee should change the password immediately when it is no longer required. Employees are reminded that it is good practice to change passwords regularly.

32. Employees must ensure that confidential information, personal data, and other sensitive information is kept secure. The security of personal data in particular is governed by the Company's Data Protection Policy, which Employees must comply with at all times when handling personal data. Workstations and screens should be locked when the Employee is away from the machine and hard copy files and documents should be secured when not in use.

33. If an Employee has been issued with a laptop, tablet, smartphone, or other mobile device, that device should be kept secure at all times, particularly when travelling. Mobile devices must be password-protected and, where more secure methods are available, such as fingerprint recognition, such methods must be used. Confidential information, personal data, and other sensitive information stored and/or accessed on a mobile device should be kept to the minimum necessary for the Employee to perform their duties. Employees should also be aware that when using mobile devices outside of the workplace, information displayed on them may be read by unauthorised third parties, for example, in public places and on public transport.

34. When opening email from external sources Employees must exercise caution in light of the risk malware, spyware, viruses, and other malicious software or code pose to system security. Employees should always ensure that they know what an attachment is before opening it. If an Employee suspects that their computer has been affected by a virus they must contact the Operations Manager immediately.

35. No equipment or device that has not been issued by the Company may be connected to or used with Company devices without the prior express permission of the Operations Manager. Such permission may be conditional on the testing and/or inspection of the equipment or device in question.

Monitoring

36. To the extent permitted or required by law, the Company may monitor Employees' use of

the Company's systems and the internet for its legitimate business purposes which include (but are not necessarily limited to) the following reasons:

- To ensure Company policies and guidelines are followed, and standards of service are maintained;
- To comply with any legal obligation;
- To investigate and prevent the unauthorised use of the Company's Internet and Communications Facilities and maintain security;
- If the Company suspects that an Employee has been spending an excessive amount of time using the Company's Internet and Communications Facilities for personal purposes.

37. Employees should be aware that all internet and email traffic data sent and received using the Company's systems is logged, including websites visited, times of visits, and duration of visits. Any personal use of the internet will necessarily therefore be logged also. Employees who wish to avoid the possibility of the Company becoming aware of any political or religious beliefs or affiliations should avoid visiting websites at work which might reveal such affiliations. By using our systems, Employees are taken to consent to personal communications being logged and monitored by the Company. The Company shall ensure that any monitoring of Employees' use of the systems complies with all relevant legislation including, but not limited to, the UK GDPR and the Human Rights Act 1998.

38. When monitoring emails, the Company will normally restrict itself to looking at the address and heading of the emails. However, if it is considered necessary, the Company may open and read emails. Employees should be aware that sensitive and confidential communications should not be sent by email because it cannot be guaranteed to be private. Employees are reminded that any permitted personal emails should be marked as "personal" in the subject line.

Recruitment

39. The Company may use internet searches to carry out due diligence as part of its recruitment process. In these circumstances, the Company will act in accordance with its equal opportunities and data protection obligations.

Misuse and Compliance

40. Any Employee found to be misusing the Company's IT equipment will be treated in line with the Disciplinary Policy. Misuse of the internet can, in some cases, amount to a criminal offence.

41. Where any evidence of misuse of the Company's IT equipment is found, the Company may undertake an investigation into the misuse in accordance with the Company's Disciplinary Policy. If criminal activity is suspected or found, the Company may hand over relevant information to the police in connection with a criminal investigation.