1. Introduction

1.1 This Communications, Email and Internet Policy applies to all employees, contractors and agents of CenCom Solutions Ltd. ("the Company") who use the communications equipment and systems provided by the Company ("Users").

1.2 Users are encouraged to use email and the internet at work as a fast and reliable method of communication with significant advantages for business.

1.3 In light of the fact that communications made by Users 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 Users and their responsibilities when using the Company's communications facilities.

1.4 "Communications facilities", "communications equipment" and "communications systems" include:

1.4.1 Telephone;

1.4.2 Fax;

1.4.3 Email;

1.4.4 Internet and Intranet;

1.4.5 Video conferencing facilities

and any other communication device or network provided by the Company.

1.5 Whilst the communications equipment and systems provided by the Company are made available to Users for the purposes of the business, a certain amount of limited personal use is permitted insofar as such personal use is consistent with this Communications Policy and the duties of the User.

2. General Principles

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 Users to:

2.1 Use communications equipment and facilities, including Company letterheads and stationery, responsibly and professionally and at all times in accordance with their duties;

2.2 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;

2.3 Ensure that they do not breach any copyright or other intellectual property right when making communications;

2.4 Ensure that they do not bind themselves or the Company to any agreement without express authority to do so;

2.5 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 conduct their use of communication systems and equipment accordingly.

3. Internet

3.1 The Company provides access to the internet for the sole purpose of business and to assist Users in the furtherance of their duties. However the Company recognises that Users may need to use the internet for personal purposes and such use is permitted provided it is reasonable and does not interfere with the User's performance of his/her duties. Users may be asked to justify the amount of time they have spent on the internet or the sites they have visited.

3.2 Users 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.

3.3 Users must not access or attempt to access any information which they know or ought to know is confidential or restricted.

3.4 Users must not download or install any software without the express permission of Cenydd Milne, The Technical Director.

3.5 Certain websites are blocked and can not be accessed from the Company's equipment or systems. If a User has a genuine and specific business need to access a blocked site he/she must contact Cenydd Milne, The Technical Director.

3.6 Users must not attempt to download, view or otherwise retrieve illegal, pornographic, sexist, racist, offensive or any other material which may cause embarrassment to the corporate image of the Company. 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.

4. Social Media

General Principles for Social Media Use

4.1 This section of the Policy exists to address the use by Users of all types of social network and social media platforms including, but not limited to, Facebook, Twitter, LinkedIn, Google+, Pinterest, Tumblr, Instagram, Yammer (collectively, "Social Media").

4.2 The purpose of this part of Policy is to minimise the various risks to the Company presented by Social Media usage.

4.3 There are certain general principles that all Users should keep in mind when using Social Media, whether for personal use or for authorised work-related purposes. The Company expects all Users to:

4.3.1 Use Social Media responsibly and professionally, and at all times in accordance with their duties;

4.3.2 Be mindful of what constitutes confidential, restricted or other proprietary information and ensure that such information is never disseminated over Social Media without the express consent of the Company

4.3.3 Ensure that their use of Social Media does not breach any other of the Company's policies including, but not limited to, its Harassment and Bullying Policy; Equal Opportunities and Diversity Policy; Disciplinary Policy and Procedure; Data Protection Policy.

4.3.4 Ensure that their use of Social Media does not breach any other laws, regulatory requirements, or other applicable rules set out by regulatory bodies and other organisations.

4.3.5 Ensure that they do not breach any copyright or other intellectual property rights when using Social Media;

4.3.6 Be mindful of the fact that any communication may be relied upon in court, to the advantage or detriment of the individual or the Company, and conduct their use of Social Media accordingly.

Personal Social Media Use

4.4 Users may use Social Media for personal purposes occasionally during work hours [for example, during breaks provided that such usage complies with the provisions of this Social Media Policy and provided that it does not interfere with their work responsibilities or productivity.

Business Social Media Use

4.5 Certain Users may from time to time be required to use Social Media on behalf of the Company. A User should only use Social Media on behalf of the Company with the authorisation of their Manager and in accordance with instructions issued by Cenydd Milne, Technical Director.

4.6 Use of Social Media for business purposes must comply with the provisions of this Social Media Policy at all times.

4.7 Users using Social Media on behalf of the Company may from time to time be required to interact with other internet users via Social Media, for example, in response to posts or enquiries regarding the Company. Unless the instructions issued to that User (see paragraph 4.5) specifically authorise the User to respond without further approval, the User may not respond to any such communications without the prior approval of Cenydd Milne, Technical Director. In any event, no User using Social Media on behalf of the Company should respond to such communications, with or without prior approval, without first consulting the relevant individual and/or department unless they are fully knowledgeable of the relevant topic and suitably qualified to respond.

4.8 Before using Social Media on behalf of the Company, Users may require training in order to do so, or may be required to demonstrate that they have already received suitable training, either from the Company or from a previous employer or other organisation.

Acceptable Use of Social Media

4.9 Unless specifically instructed to do so, Users should make it clear that they are posting on Social Media as themselves, not as the Company, and that all views expressed on Social Media by that User are the author's own and do not necessarily reflect the views of the Company.

4.10 Unless using Social Media on behalf of the Company, Users should not use any Social Media accounts belonging to, or otherwise associated with, the Company.

4.11 Company email addresses may only be used to sign up to Social Media websites for work-related purposes.

4.12 Users should always be respectful to others when using Social Media and should always be mindful of the fact that their association with the Company may be known to anyone at any time. The conduct of all Users on Social Media may reflect on the Company, whether positive or negative. This applies whether a User is using Social Media for business purposes or for personal purposes, whether during workings hours or otherwise.

4.13 If a User is unsure as to the appropriateness of a post or any other Social Media activity

with respect to this Social Media Policy, they should consult Cenydd Milne, Technical Director before continuing.

Unacceptable and Prohibited Use of Social Media

4.14 Users must not use Social Media to defame or otherwise disparage the Company or any of its employees, contractors, agents, or other affiliated third parties and organisations.

4.15 Users must ensure that their use of Social Media does not damage the Company, its interests, or its reputation, whether directly or indirectly, in any way.

4.16 As under paragraph 4.9, unless specifically instructed to do so, Users must not represent themselves on Social Media as the Company or as posting on behalf of the Company.

4.17 Users may not share confidential, commercially sensitive or other proprietary business information belonging to the Company or any of its employees, contractors, agents, or other affiliated third parties and organisations on Social Media unless specifically authorised to do so by Cenydd Milne, Technical Director.

4.18 Users may not use any intellectual property belonging to the Company on Social Media (including, but not limited to, trade marks and logos) unless specifically authorised to do so by Cenydd Milne, Techical Director.

4.19 Users may not add contacts made during the course of their duties to their personal Social Media accounts without the authorisation of Cenydd Milne, Technical Director.

Recruitment

4.20 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.

5. Email

Company Email

5.1 The email address with which Users are provided by the Company (ending in the suffix "@cencom.co.uk") is provided for business purposes in order to facilitate information sharing and timely communication with Clients, Colleagues, Suppliers and associated 3rd parties. Any Company business which is conducted via email must be conducted through the Company email and is under no circumstances to be conducted through any other personal email address or account.

5.2 Users should adopt the following points as part of best practice:

5.2.1 Before communicating via email, Users should satisfy themselves that it is the most suitable mode of communication, particularly where time is of the essence;

5.2.2 Ensure that the email contains the Company disclaimer notice. This should be added automatically by the email client. If it is not, Users should speak to Cenydd Milne, Technical Director immediately;

5.2.3 All emails should contain the appropriate business reference(s), either in the subject line or in the body of the text;

5.2.4 Emails should be worded appropriately and in the same professional manner as if they were a letter;

5.2.5 Users should be careful not to copy an email automatically to everyone copied in to the original message to which they are responding as this may result in inappropriate disclosure of confidential information;

5.2.6 All emails should be proof read 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;

5.2.7 If an important document is transmitted vie email, the sender should telephone the recipient to confirm that the document has been received in full;

5.2.8 If any email contains sensitive information it should be marked as confidential and have its contents encrypted to ensure secure comminication

5.3 Users must not email any business document to their own or a colleague's personal web-based email accounts. Further Users must not email any business document to any clients or suppliers web-based email address unless specifically permitted to do so by them.

5.4 The Company recognises that there may be instances where Users may need to use their Company email address for personal reasons. This is permitted on the condition that such use is kept to a minimum and does not interfere with the performance of the User's duties. In any case Users are not permitted to use their Company email address to subscribe to any newsletters or to receive any marketing.

5.5 If Users do use the 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 Part 9 of this policy.

5.6 Users 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. Users should remember that data which appears to have been deleted is often recoverable.

Personal Email

5.7 Users 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 User's performance of his/her duties

6. Telephone Use

Company Telephone System

6.1 The Company's telephone lines are for the exclusive use by Users working on the Company's business. Essential personal telephone calls regarding Users' domestic arrangements are acceptable, but excessive use of the Company's telephone system for personal calls is prohibited. Acceptable telephone use may be defined as no more than five minutes of personal calls in a working day. Any personal telephone calls should be timed to cause minimal disruption to Users' work.

6.2 Users should be aware that telephone calls made and received on the Company's telephone system may be routinely monitored to ensure customer satisfaction or to check the telephone system is not being abused.

6.3 If the Company discovers that the telephone system has been used excessively for personal calls, this will be dealt with under the Company's disciplinary procedures.

Mobile phones

6.4 Essential personal telephone calls regarding Users' domestic arrangements are acceptable but excessive use of Users' own mobile phones for personal calls (also texting, emailing and web browsing) is prohibited. In order to avoid disruption to others, mobile phones should be set to silent during normal working hours.

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

7. Security

7.1 The integrity of the Company's business relies on the security of its communications equipment and systems. Users bear the responsibility of preserving the security of communications equipment and systems through careful and cautious use.

7.2 Access to certain websites is blocked from Company communications equipment and systems. Often the decision to block a website is based on potential security risks that the site poses. Users must not attempt to circumvent any blocks placed on any website or features by the Company.

7.3 Users must not download or install any software or program without the express permission of Cenydd Milne, Technical Director, and are reminded of paragraphs 3.2 and 3.4 of this policy.

7.4 Users must not share any password that they use for accessing Company communications equipment and systems with any person, other than when it is necessary for maintenance or repairs by support staff. Where it has been necessary to share a password, the User should change the password immediately when it is no longer required by Support Staff. Users are reminded that it is good practice to change passwords regularly.

7.5 Users must ensure that confidential and sensitive information is kept secure. Workstations and screens should be locked when the User is away from the machine, hard copy files and documents should be secured when not in use and caution should be exercised when using mobile telephones outside of the workplace.

7.6 Some systems require the use of Dual or Multifactor Authentication to logon, these systems require an app to be installed on your personal device to provide the second code. If you lose, break or leave your device somewhere you should notify Cenydd Milne, Technical Director immediately.

7.7 When opening email from external sources Users must exercise caution in light of the risk viruses pose to system security. Users should always ensure that they know what an attachment is before opening it. If a User suspects that their computer has been affected by a virus they must contact Cenydd Milne, Technical Directly immediately.

7.8 No external equipment or device may be connected to or used in conjunction with the Company's equipment or systems without the prior express permission of Cenydd Milne, Technical Director.

8. Monitoring

8.1 The Company may monitor Users' communications for the following reasons:

8.1.1 To ensure Company policies and guidelines are followed, and standards of service are maintained;

8.1.2 To provide evidence of transactions and communications;

8.1.3 To help combat unauthorised use of the Company's communications equipment and systems and maintain security;

8.1.4 If the Company suspects that a User has been viewing or sending offensive or illegal material (including but not limited to that which breaches another party's intellectual property rights);

8.1.5 If the Company suspects that a User has been spending an excessive amount of time viewing non work-related sites (including, but not limited to, Social Media) and/or sending and receiving an excessive number of personal emails;

8.1.6 In order to better understand the requirements of the Company in terms of the provision of communications equipment and systems.

8.2 Users should be aware that all internet and email traffic data sent and received using the Company's communication systems is logged, including websites visited, times of visits and duration of visits. Any personal use of the internet, including but not limited to Social Media, will therefore be logged also, irrespective of whether or not it is in compliance with this Policy and other Company Policies. Users 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 the Company's communications equipment and systems for personal use, Users are taken to consent to personal communications being logged and monitored by the Company. The Company shall ensure that any monitoring of communications complies with the General Data Protection Regulation GDPR, the Regulation of Investigatory Powers Act 2000, and the Human Rights act 1998.

8.3 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. Users should be aware that sensitive and confidential communications should not be sent by email because it cannot be guaranteed to be private.

9. Misuse and Compliance

9.1 Any User found to be misusing the communications equipment and systems provided by the Company will be treated in line with the usual disciplinary procedure.

9.2 The viewing, transmission, downloading, uploading or accessing in any way of any of the following material using Company communications equipment and systems will amount to gross misconduct with the possibility of summary dismissal:

9.2.1 Material which is pornographic, sexist, racist, homophobic, paedophilic or any other discriminatory or otherwise offensive material;

9.2.2 Illegal or criminal material, including material which breaches copyright or any other intellectual property right;

9.2.3 Any material which has the object or effect of causing harassment to the recipient;

9.2.4 Material which the User knows, or ought to know, is confidential or restricted information and which they are not authorised to deal with;

9.2.5 Any website which the Company has blocked access to from CenCom Soltuions Ltd. communications equipment and systems.

9.3 Any questions regarding this Policy should be referred to Cenydd Milne, Technical Director, cenydd@cencom.co.uk.

9.4 If any User becomes aware of any content online that reflects poorly on the Company or otherwise defames or disparages the Company, they should contact Cenydd Milne,

Technical Director, cenydd@cencom.co.uk.

This policy has been approved & authorised by:

Name:	Cenydd Milne
Position:	Technical Director
Date:	01/04/2018
Signature:	