1300 761 761
www.csw-it.com.au
info@csw-it.com.au
430 Collins Street,
Melbourne, VIC, 3000
ABN: 46 610 716 919

Internet and Email Policy

CSW ICT Policy (POL) for:			Internet and Email Policy
SOP Number:	POL11	Version Number:	1.2
Effective Date:	1 Jan 2025	Last Review Date:	14 Apr 2025
Author:	Tristan Chen	Next Review Date:	January 2026
Reviewer	Exec/GM		

Revision History			
Version	Description	Author	Date
0.1	Draft	Tristan Chen	Jan 25
1.0	Initial Version	Tristan Chen	Jan 25
1.1	Various updates and inclusions	Tristan Chen	Feb 25
1.2	Reviewed for Website Publishing	Soren Walker	Apr 23

Purpose and Objective:
Details on the CSW-IT Internet and Email Policy.

References:

1 Introduction

1.1 Clear Corporate Technology Pty Ltd ("**the Company**") recognises that its computer, email and internet resources are critical tools of the Company workplace, however there are a number of serious risks or consequences that may affect the Company, its employees or customers if these resources are misused.

1.2 This policy sets out the appropriate standard of behaviour for users of the Company's computer, email and internet resources and should be read in line with the Company's Workplace Surveillance and Social Media Policies.

2 Scope

2.1 This policy applies to all users who access or use the Company's computer, email and internet resources, including but not limited to employees, contractors, consultants, volunteers and those performing work experience ("**Users**").

3 Use of Computer Email and Internet Resources

3.1 Users are entitled to access and use the Company's computer, email and internet resources for business purposes.

3.2 Limited private use of the Company's computer, email and internet resources is permitted subject to the following conditions:

i. private use must be kept to a minimum;

ii. private use must not interfere with or delay a User's work obligations in any way; and

iii. private use must comply with all Company policies and must not be inconsistent with the User's contract of employment or contractor agreement.

4 Material

4.1 The display or transmission of offensive or sexually explicit material is unacceptable and will not be tolerated. The transmission of any such material by Users, even if sent from outside sources, is strictly forbidden and may lead to immediate termination of employment or engagement.

4.2 All computers and the data stored on them are and remain at all times, the property of the Company. As such, all email messages composed, sent, and/or received are the property of the Company.

5 Inappropriate Use

5.1 Examples of inappropriate use of Company computer, email and internet resources include (but are not limited to):

i. use for unlawful activities (e.g. hacking or intellectual property piracy);

ii. use for activities that create an actual or potential conflict with the user's obligations to the Company (e.g. sending sensitive information to a competitor);

iii. use of abusive language or graphics in either public or private messages;

iv. activities which could cause congestion and/or disruption of networks or systems (e.g. downloading large media files); and

v. accessing, viewing, posting, downloading, storing, transmitting, sharing, printing, distributing or soliciting of any information or material that the Company views as racist, pornographic, obscene, abusive or otherwise offensive.

5.2 Email messages must not contain material that is or could reasonably be considered offensive, defamatory, discriminatory or derogatory. Such inappropriate content would include, but is not limited to:

i. sexual comments or images;

ii. solicitation of non-business causes (including but not limited to political, religious causes unless the activity is a company sponsored or sanctioned activity);

iii. chain-letters;

iv. gender-specific comments, or any comments that might offend someone on account of his or her age, gender, sexual orientation, religious or political beliefs, national origin or disability; and

v. messages which have the potential to be viewed as defamatory, threatening or obscene.

6 Security

6.1 Email does not possess a guarantee of security. Where possible, highly sensitive or confidential documents should not be sent via email. If in doubt, a User must check with his or her manager.

7 Monitoring Activities

7.1 The Company reserves the right to monitor (log) email and internet use in order to maintain the standards set out in this policy and the security of our computer system. Senior managers of the Company have the right to access information so logged.

7.2 System administrators and senior management have access to individual audit trails of email and internet use for necessary maintenance of the computer system. The Company has the ability to monitor the use and operation of the Company computer resources by means of software designed to filter the use of internet and email content and to monitor compliance with the Company's policies. The Company may conduct forensic computer examinations randomly and in the event of a suspected breach of policy.

7.3 Monitoring by the Company may take place on a continuous and ongoing basis. Employees should therefore assume that all email correspondence may be opened by Company management.

8 Restricting or Blocking Access

8.1 The Company may, at any time and without notifying Users, restrict or block access to various

internet sites and applications.

8.2 Any use of programs by Users to in any way subvert the Company's filters in order to access blocked internet sites and/or applications will amount to a breach of this Policy.

9 Protocols

9.1 Users must ensure that the form and content of work-related emails are drafted in a professional and appropriate manner.

9.2 Similarly, consideration should be given to the distribution of a message and only relevant parties should be included as the addressees or be copied-in.

9.3 Emails should be written in sentence case rather than capitals. Capital letters appear threatening and unfriendly and tend to create an adverse impression.

10 Formal Business Records

10.1 Depending on its content, an email message may constitute a formal business record. If this is the case, the user who sends or receives the message must ensure the message is stored in an appropriate place (e.g. electronic or hard copy file).

11 Breach of this Policy

11.1 Any User who is found to have breached this policy may be subject to disciplinary action, up to and including termination of employment or engagement.