

Acceptable Use of IT Systems Policy

Consultus Services Pvt Ltd **| 19 Glenara avenue, harare, zimbabwe**

**Consultus Publishing Services**

 **Information Technology**

**Acceptable Use of IT Systems Policy**

|  |
| --- |
| **Description** |
| **Title** | Acceptable Use of IT Systems Policy |
| **Policy number** | CPS/003/2020 |
| **Effective date** | TBA |
| **Review Date** | TBA |

**Policy Owner:** General Manager

**Department:** Administration

#

**SUMMARY/OVERVIEW OF PERMISSIBLE USE**

|  |  |
| --- | --- |
| IT Systems **MAY ONLY** be used for | * CPS Business
* Approved, limited and appropriate Personal Use
 |
|  |
| IT Systems may be used for Limited Personal Use, **PROVIDED THAT** | * Approval is granted by OE and permission from CEO
* Meets the guidelines herein
* Is approved for your business use
 |
|  |  |
| IT Systems **MAY NOT** be used for | * Non-Business Videos
* Non-Business Photos
* Non-Business Audio
* Any activity that breaches any legislation or any activity that is illegal
* Sending, forwarding or storing any emails, documents or files that
	+ Breach copyright
	+ Contain
		- Pornography material or
		- Obscene language
		- Racial or any other derogatory comments
* Hacking or gaming
* Downloading software
* Advertising goods and services related to non-CPS commercial purposes
* Chain letters
* Third party instant messaging applications
* Anything that might bring CPS into disrepute
 |

#

#  Summary

CPS Acceptable Use of Information Systems Policy defines appropriate and inappropriate use of CPS Information Systems.

CPS Information Systems include devices, services (e.g. Internet, email, “bring your own device” (when connected to CPS systems) and telephony), applications and information in logical and physical form as well as any other CPS equipment. This also extends to service providers’ systems/equipment when provided to CPS.

Inappropriate use of CPS Information Systems exposes CPS to information security risks, such as unauthorised access, corruption, loss of information, compromise to our network systems and services. These risks could result in reputational damage for CPS as well as fines and/or claims for damages resulting from a breach of legislative or contractual obligations

It is important that you understand what is required of you and what you need to do to comply with this policy. You must be aware of your responsibilities and understand that failure to comply with this policy may result in disciplinary action being taken against you including dismissal and/or legal action.

## Audience

This policy applies to all CPS employees and anyone that has access to CPS Information Systems, however they are employed or under a term of contract with CPS, including via third parties. It also extends to information held on behalf of third parties and partners.

# Key points of this policy

### Phishing

**You must** be vigilant when opening attachments or clicking on links in any communications you receive. CPS is often targeted by scam emails (phishing) which may introduce malicious software or trick you into giving up confidential information e.g. your personal credentials.

### Personal Communication

**You are** allowed reasonable and limited personal use when using CPS Information Systems however; they must not be used to take part in online gambling and all personal use is done at your own risk. CPS may decide to limit your ability to use CPS Information Systems for personal use where there is possible, or actual, interference with CPS business. This would be decided by your line manager with input from CPS MC.

**You must not** use a personal email account (such as Gmail, Hotmail etc.) for your CPS work. Secure options for accessing your CPS email on the go or at home are available.

**You must not** use your CPS email address to sign up for or link to any external service that will be used for personal reasons. External services include (but are not limited to) banking, shopping, social media, cloud services etc. See Sections 2, 5 and 10 for further details on personal use of CPS Information Systems.

### Offensive Material

**You must not** knowingly attempt to visit, send or store any website, electronic communications or information on CPS Information Systems that is likely to cause harassment, alarm or distress. This includes sites and information which may contain nudity, pornographic, obscene, indecent, hateful or other offensive material. See Section 2.8: Offensive Material for further details.

### Reporting Theft or Loss

Be vigilant and look after CPS equipment and information when you’re in the office or out and about. **You must** report all lost or stolen CPS Information Systems, or other devices containing CPS information, to your Supervisor or Line Manager. Where the theft or loss of a physical item involves **personal information** then you must also immediately report the incident to the General Manager.

### Monitoring

**You must** understand that CPS may monitor your use of CPS Information Systems for security purposes and to check your compliance with this policy at any time and potentially without notifying you. See section 11: Monitoring of CPS Information Systems for further details.

**TABLE OF CONTENTS**

1. [Introduction 6](#_TOC_250022)
	1. [Purpose 6](#_TOC_250021)
	2. [Audience 6](#_TOC_250020)
	3. [Scope 7](#_TOC_250019)
2. [General Use of CPS Information Systems 7](#_TOC_250018)
	1. Your Behaviour 7
	2. Your Role 7
	3. Information Security Incidents 7
	4. Business Use 7
	5. Personal Use 7
	6. Information Privacy 7
	7. Accessing CPS Information Systems 7
	8. Offensive Material 8
	9. Actions Upon Termination of Contract 8
3. [PROTECTED and RESTRICTED Information 8](#_TOC_250017)
	1. Working with PROTECTED 8
4. [Secure Use of the Internet 8](#_TOC_250016)
	1. Unauthorised Software 8
	2. Mobile Applications 9
	3. Social Networking Sites 9
	4. Remote Access 9
5. [Secure Use of electronic Communications 9](#_TOC_250015)
	1. Sending PROTECTED or RESTRICTED Information 9
	2. Use of Personal Communication Accounts 9
	3. Use of CPS Email Address 9
	4. Unnecessary Email Traffic 10
	5. Suspect Email Messages 10
	6. E-mail Auto-Forwarding 10
6. [Physical Security 10](#_TOC_250014)
	1. Access to Premises 10
	2. Keeping Your Desk Clear 10
	3. Protecting Your Equipment 10
	4. Safe Storage 10
	5. Shoulder Surfing 10
	6. Protecting Your Screen 11
	7. Shutting Down Your Computer 11
	8. Reporting Theft or Loss 11
7. [Passwords 11](#_TOC_250013)
	1. Creation of Strong Passwords 11
	2. Keep Passwords Secure 11
	3. Exemptions and Delegated Authority 11
8. [Removable Storage Media 11](#_TOC_250012)
	1. Using removable storage 11
	2. Removable Media from Third Parties 11
9. [Secure Configurations of CPS Information Systems 12](#_TOC_250011)
	1. Security Tools on CPS Information System 12
	2. Configuration of CPS Information Systems 12
	3. Authorised Information Systems 12
10. [Communications Services 12](#_TOC_250010)
	1. Personal Use 12
11. [Monitoring of CPS Information Systems 12](#_TOC_250009)
	1. General Monitoring 12
	2. Specific Monitoring 12
	3. Monitoring Personnel 13
	4. Authority to Monitor 13
12. [Investigation of Individuals Using CPS Information Systems 13](#_TOC_250008)
	1. Investigating Your Use of CPS Information Systems 13
	2. Investigation of Past Communications 13
	3. Notification of Investigations 14
	4. Personal Information During Investigations 14
13. [Defamation 14](#_TOC_250007)
	1. What is Defamation 14
	2. Defamation is Not Allowed 14
14. [Harassment 14](#_TOC_250006)
	1. Harassment is Prohibited 14
15. [Copyright 14](#_TOC_250005)
	1. Protecting Copyright 14
16. [Exception Management 15](#_TOC_250004)
	1. Exceptions Process 15
17. [Policy Review 15](#_TOC_250003)
	1. Amendments 15
18. [Definitions 16](#_TOC_250002)
19. [References 17](#_TOC_250001)
20. [Document control 19](#_TOC_250000)

**CPS Acceptable Use of Information Systems Policy**

## Introduction

Information is an asset, and like any other business asset it has a value and must be protected. This value is not just financial but is based on the consequences of the information or Information Systems, being compromised and the negative impact that would have on individuals and CPS. CPS will continue to protect its interests against the inappropriate use of its Information Systems.

For this policy, Information Systems is defined as CPS systems, devices, services (e.g. Internet, email, “bring your own device” (when connected to CPS systems) and telephony), applications and information in logical and physical form as well as any other CPS equipment. This also includes service providers’ systems/equipment when provided to CPS.

CPS will provide the appropriate IT equipment and/or access rights required for you to meet the objectives of your role; CPS expects you to be careful with that equipment and to make sure it isn’t damaged, misused, lost or stolen. See [CPS HR Document](https://intranet.gateway.bbc.co.uk/whatshappening/Pages/bbc_code_of_conduct--.aspx) for further Information.

This Acceptable Use of Information Systems policy is part of the Information Security Policy Framework and should be read in conjunction with any other relevant policies as mentioned in this document.

It is not the intention of this policy to impose unnecessary restrictions on you that conflict with CPS’s culture of openness, trust and integrity. However, your awareness and co-operation is essential for maintaining the effective security of CPS Information Systems.

### Purpose

This policy has been written to help you understand what CPS defines as appropriate and inappropriate use of its Information Systems and to remain within those limits during your work with CPS. Inappropriate use exposes CPS to risks such as malware attacks, inappropriate or unauthorised access, corruption, loss or disclosure of information, or a compromise of network systems and services. These risks could result in public embarrassment for CPS as well as fines and/or claims for damages resulting from a breach of legislative or contractual obligations.

It is important that you understand what is required of you and what you need to do to comply with this policy. You must be aware of your responsibilities and understand that failure to comply with this policy may result in disciplinary action being taken against you including dismissal and/or legal action.

If you have any questions about this policy, please contact your line manager first.

### Audience

This policy applies always when using CPS Information Systems and not just during your normal working hours.

This policy applies to anyone who has access to CPS Information Systems however they are employed or under a term of contract with CPS, including via third parties. In effect, this policy applies to anyone working in CPS Group regardless of your location. It also extends to information held on behalf of third parties and partners.

### Scope

This policy applies to all CPS Information Systems as well as to any other device used to store or process CPS information. This policy also applies when using your own device to store, access or process information on CPS Information Systems.

## General Use of CPS Information Systems

* 1. **Your Behaviour:** You must act honestly and with integrity at all times to protect CPS’s reputation, in accordance with CPS values.
	2. **Your Role:** You must understand your role and responsibilities with regard to CPS Information Systems. If this is unclear then you must consult your line manager.
	3. **Information Security Incidents:** You must report all actual or suspected information security incidents immediately to the [General Manager](https://intranet.gateway.bbc.co.uk/fo/workplace-and-information-rights/Pages/Data-Protection-Breaches.aspx).
	4. **Business Use:** You must not use CPS Information Systems for any business activities which are not related to your work at CPS.
	5. **Personal Use:** You are allowed reasonable and limited personal use when using CPS Information Systems however; they must not be used to take part in online gambling. CPS may decide to limit your ability to use CPS Information Systems for personal use where there is possible, or actual, interference with CPS business. This would be decided by your line manager with input from CPS Management Committee. Any personal use of CPS Information Systems is at your own risk.
	6. **Information Privacy:** Your personal privacy is respected and access controls are in place, but you must understand that CPS may monitor your use of CPS Information Systems for security purposes and also to check your compliance with this policy at any time and potentially without notifying you. Please see the section 11: Monitoring for further details.
	7. **Accessing CPS Information Systems:** When accessing CPS Information Systems you must only carry out the activities you are authorised to do. You must not access or try to access any CPS Information Systems where you are not authorised to do so, for example logging into accounts which are not yours. Doing so may be a crime.

You are responsible for any activity carried out under your username. You must not let anyone else use your CPS Information System when logged in with your own username and password unless all the following apply:

* + - it is for IT support or delivering presentations/training where multiple people need to use one device;
		- it is for a limited period of time; and
		- it takes place under your direct and continuous supervision.
	1. **Offensive Material:** You must not knowingly attempt to visit, send or store any website, electronic communications or information on CPS Information Systems that is likely to cause harassment, alarm or distress. This includes sites and information which may contain nudity, pornographic, obscene, indecent, hateful or other offensive material. Authorisation to access such material for research or publishing purposes must be applied for through the Publishing Manager, and ultimate permission granted by the CEO.
	2. **Actions Upon Termination of Contract:** CPS equipment and data, for example, but not limited to, laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to CPS at termination of contract. All CPS data or intellectual property created, developed or used by the employee during the period of his/her employment remains the property of CPS and must not be retained beyond termination or reused for any other purpose unless otherwise agreed by CPS. Team and line managers are responsible for ensuring this is carried out alongside with any IT access to CPS Information Systems.

## PROTECTED and RESTRICTED Information

* 1. **Working with PROTECTED** and **RESTRICTED Information:** You must not print, share, post, publish, upload or email any information that is likely to be, or has already been classified as **PROTECTED** or **RESTRICTED** information unless you are required to do so. If you need to handle **PROTECTED** or **RESTRICTED** information then you must take the appropriate measures to maintain its confidentiality, e.g. by using encryption or ensuring its physical security.

## Secure Use of the Internet

* 1. **Unauthorised Software:** The integrity and security of CPS and its Information Systems could be impacted by downloading unauthorised, illegal or malicious software. You must not knowingly download, install or run any software on CPS Information Systems without first obtaining appropriate authorisation (for example by contacting your Supervisor or Line Manager), unless the software is listed as approved on the Software Catalogue. If you need to install software you must contact the General Manager. When this is not possible (for example outside normal working hours) they must inform their supervisors or managers

 by e-mail and ensure that the software is removed immediately after the specific task is completed.

* 1. **Mobile Applications:** You must only download or install mobile applications onto CPS Information Systems from approved and reputable sources. The integrity and security of CPS and its Information Systems could be impacted by downloading unauthorised, illegal or malicious software.

You must read the information about an application in the application store before you download it and make sure that you are happy with the information it will be accessing. Any non-CPS application that wants to capture CPS information and store it must not be used. If you are in any doubt about whether to download an application, please contact the IT Administrator or General Manager.

* 1. **Social Networking Sites:** You must use caution when using social networking for communication. You must use social networking sites in a professional and responsible manner and your contributions must comply with the Social Media and Social Networking statements within CPS.

It is your responsibility to ensure the social media account is protected by enabling the privacy settings available.

* 1. **Remote Access:** When you use a public/shared device to access CPS information remotely, you must reject any prompt to save your username or password in the browser for future use. You must also ensure that you log out of the remote access service completely when you are finished and close any open browser. Where possible you should log out of the device completely and either shut it down or restart the device. It is your responsibility to ensure that your remote access occurs in an appropriate environment.

## Secure Use of electronic Communications

* 1. **Sending PROTECTED or RESTRICTED Information:** If you need to communicate any **PROTECTED** information then encryption may be required. Encryption must be in place for any personal and/or **RESTRICTED** information.
	2. **Use of Personal Communication Accounts:** You must not send or forward any **PROTECTED** or **RESTRICTED** information to your personal communication systems (such as instant messaging, email, video communications), or use such an account for CPS business. If you have a requirement to work from home you should use a CPS approved remote working solution from your Supervisor or Line Manager.
	3. **Use of CPS Email Address:** You must not use your CPS email address to sign up for or link to any external service that will be used for personal reasons. External services include (but are not limited to) banking, shopping, social media, cloud services etc.
	4. **Unnecessary Email Traffic:** You should not forward chain and spam communications as these cause unnecessary congestion on the network and also take up storage space.

You should also take great care before using “Reply All” to e-mail as this can generate very high levels of unnecessary traffic, or can lead to the distribution of sensitive information to recipients who do not have a legitimate reason to see it. Only use “Reply All” if every person copied into the email needs to receive it.

* 1. **Suspect Email Messages:** CPS is often targeted by suspicious emails which may introduce malicious software or trick you into giving up confidential information (phishing)

e.g. your password, username or banking details. You must be careful when opening attachments or clicking on links in any communications you receive. This applies to emails from unknown sources, or unexpected communications from known sources.

* 1. **E-mail Auto-Forwarding:** E-mail auto-forwarding to external addresses is not permitted from a CPS e-mail account unless an approved exception is authorised by the General Manager. Such an exception will only be granted for clear and compelling business reasons, and where all alternatives have been considered carefully and proved inappropriate.

## Physical Security

* 1. **Access to Premises:** Access to CPS premises is for authorised personnel only. Please be aware of those in your office area and report any suspicious behaviour to on duty security officers. Access to CPS premises may be recorded for security purposes. Any attempted unauthorised access to areas which are restricted for either security or health and safety reasons is a violation of this policy.
	2. **Keeping Your Desk Clear:** You must make sure all **PROTECTED** and **RESTRICTED** information is locked away when you leave the office in accordance with CPS’s clear desk policy.
	3. **Protecting Your Equipment:** You are responsible for ensuring the security and safe keeping of CPS Information Systems and other devices containing CPS information; particularly at non-CPS locations such as your vehicle, at home, when on public transportation, having a coffee etc.
	4. **Safe Storage:** If you need to leave any portable CPS Information System (such as phones, mobiles, laptops and tablets), or any other device containing CPS information, in the office overnight or when you have finished working for the day, then you must lock it into storage. If you are at a non-CPS location then you must take similar measures.
	5. **Shoulder Surfing:** In public places, such as buses or coffee shops, you must be aware of others who may be able to view your password entry, screen or papers. You must take

appropriate precautions particularly with using **PROTECTED** or **RESTRICTED** information in such circumstances.

* 1. **Protecting Your Screen:** If you need to leave CPS Information Systems, or other devices containing CPS information, unattended then you must activate a password protected screen lock.
	2. **Shutting Down Your Computer:** You must always shut down your computer, and wait until it has fully shut-down, when you have to leave it unattended for long periods of time or when not using it outside of your normal working hours.
	3. **Reporting Theft or Loss:** You must immediately report all lost or stolen CPS Information Systems, or other devices containing CPS information, to your Supervisor or Line Manager and by following the link in the references section. Where the theft or loss of a physical item involves personal information then you must also immediately report the incident to contact the General Manager as per the link in the references section.

## Passwords

* 1. **Creation of Strong Passwords:** You must create your unique passwords
	2. **Keep Passwords Secure:** You must keep all your passwords safe. Don’t write them down in any manner that would make it easy to decipher and don’t tell anyone your login details or password – including your manager or IT Administrator. This includes all information systems and websites i.e. social media. Any activity carried out on your password protected account will be deemed to be your activity unless there is evidence to the contrary.
	3. **Exemptions and Delegated Authority:** We recognise there may be instances when you do need to share your password, however you must only do this with a valid business justification. You must thereafter change your password at the earliest opportunity.

## Removable Storage Media

* 1. **Using removable storage:** If you are copying **PROTECTED** information to removable storage media (e.g. USB drives, CD/ DVDs etc.) then encryption is recommended. If you are copying personal which is **PROTECTED** and/or **RESTRICTED** information, then you **must encrypt** it and keep it secure at all times.
	2. **Removable Media from Third Parties:** You must advise any third party wishing to send you any **personal or RESTRICTED** information on removable media to use encryptio. If you have received the removable media unencrypted then you must copy the information to your CPS Information System and immediately encrypt the removable media using CPS.

## Secure Configurations of CPS Information Systems

* 1. **Security Tools on CPS Information System:** You must not attempt to bypass or tamper with any of the security measures that CPS has in place.
	2. **Configuration of CPS Information Systems:** You must not modify the configuration of CPS Information Systems nor install additional software unless you have been authorised to do so.
	3. **Authorised Information Systems:** Only equipment and media (including removable storage media) that has been authorised by CPS must be used to directly connect to CPS Information Systems, including the network.

## Communications Services

* 1. **Personal Use:** You are permitted to use CPS’s communications services, including but not limited to telephones, mobile phones and Skype, for a reasonable and limited personal use, however this must be kept to a minimum since the communication services must be kept available for business use. Any abuse of the communications service, such as excessive, long, premium or long-distance usage may result in disciplinary action. If you have an exceptional circumstance then you must seek authorisation from your line manager.

## Social Media

* 1. **See Appendix 2: Social Media Policy**

## Monitoring of CPS Information Systems

* 1. **General Monitoring:** Both specialist IT Administrators, designated staff and automated computerised systems are used to monitor CPS Information Systems including but not limited to CPS telephones, mobile devices, computers, CCTV, communications systems and Internet systems. Systems have been implemented to automate monitoring where viable to ensure real-time protection and minimal human intervention. Digital information and data passing through these systems are subject to on-going and random monitoring for system security and integrity reasons in order to:
		+ maintain the effective operation of CPS’s communications systems;
		+ check on standards of service and quality of staff performance; and
		+ ensure compliance with this policy.
	2. **Specific Monitoring:** Your communications may be monitored when it appears that CPS Information Systems are being misused or used inappropriately. There may be other reasons why your communications are monitored, e.g. in your absence after a formal request is made for access to emails and/or data files in your mailbox or on your device to ensure business correspondence is dealt with.
	3. **Monitoring Personnel:** Access to information obtained through monitoring is controlled and limited to trained and designated staff to ensure an acceptable level of confidentiality and privacy.

## Investigation of Individuals Using CPS Information Systems

* 1. **Investigating Your Use of CPS Information Systems:** CPS respects your privacy and does not investigate your activity on CPS Information Systems without proper grounds. CPS however is ultimately responsible for all communications and devices on CPS Information Systems. It is therefore important that you understand that CPS can investigate your CPS communications and your use of its Information Systems for reasons which include:
		+ any serious incident where the investigation of CPS, or its staff, is necessary in the public interest;
		+ to comply with legal obligations and the prevention or detection of criminal activities;
		+ to ensure that CPS’s policies and procedures are adhered to;
		+ to prevent or detect unauthorised use of CPS Information Systems; and
		+ when necessary, to conduct authorised investigations into an individual user.
	2. **Investigation of Past Communications:** Your past communications may be examined or analysed as part of on-going operational needs or investigations. CPS may use any

information it obtains via this process to investigate any claims of breach of this policy or any law and to instigate appropriate disciplinary or legal proceedings.

* 1. **Notification of Investigations:** Wherever reasonable, and if appropriate, we will consult you about any suspected breach of this policy before any action is taken against you. However, it may not be practical to consult with you beforehand where illegal behaviour or gross misconduct is suspected.
	2. **Personal Information During Investigations:** You should be aware that investigations may reveal personal information about you, for instance which websites you visit, the identity of people you email for personal reasons etc. This will be held in confidence unless it is needed to form part of an authorised investigation.

## Defamation

* 1. **What is Defamation**: Defamation is the publication of a statement that adversely affects the reputation of a person or an organisation. The publication can be made using the Internet or any other electronic communication.
	2. **Defamation is Not Allowed:** You must not send or circulate, internally or externally, any information that is defamatory. This includes any information that contains negative comments about an individual or organisation without first checking that the contents of the information are accurate. A person or organisation defamed can sue you or CPS for damages. Although the law recognises that it is a defence if the information is ‘true’, the onus is on you or CPS to show that.

## Harassment

* 1. **Harassment is Prohibited:** CPS will not tolerate any form of harassment and is committed to providing a workplace in which the dignity of individuals is respected. You must not knowingly attempt to send electronic communications or information on CPS Information Systems which may be deemed by the recipient to violate dignity or be perceived as intimidating, hostile, degrading, humiliating or offensive. Any harassment will be dealt with under CPS and may result in disciplinary action being taken and could potentially be a criminal offence.

## Copyright

* 1. **Protecting Copyright:** You must not download, store, copy or transmit the works of others without their permission as this may infringe copyright. If you use someone else’s copyright protected material without their consent.

## Exception Management

* 1. **Exceptions Process:** Where it is not possible to apply or enforce any part of this policy then a written communication must be made to the General Manager who will review the business justification and advice on the risks involved. Policy exceptions will only be issued when the Data Owner has signed off on the identified risks.

## Policy Review

* 1. **Amendments:** CPS reserves the right to review and amend this policy on a regular basis.

## Appendix 1: Document control

|  |  |
| --- | --- |
| **Author** | **CPS Information Security** |
| **Document Name** | Acceptable Use of Information Systems Policy |
| **Version** | 2.0 |
| **Source** | CPS Information Security |
| **Policy Owner(s)** | HR&CIP Committee of the Board of Directors |
| **Date** | **Version** | **Author** | **Changes/Comments** |
| **1/07/2013** | 1.0 |  | First version (adopted from Longman Zimbabwe) |
| **1/10/18** | 2.0 | Masimba Tinashe Madondo | Updated following recommendation by HRCIP committee |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

##