

COMMUNICATIONS POLICY

This policy document regarding Internet usage is part of the terms and conditions of employment of *organisation name*, ("the Organisation").

This policy applies to your employees at all other Organisation sites that you manage. This policy must also be observed at all client facilities. Employees must also comply with policies that exist at client or partner sites.

Please note that this policy also applies to contractors, agency worker, temporary staff and the Organisation.

For any policy to be effective it must be understood and apply to all staff regardless of location.

If you have any questions regarding this policy you please consult *[Insert manager name]* before taking any action that may breach this policy.

1. Minor Breaches

Minor breaches of this policy shall be dealt with using the disciplinary procedure.

2. Serious Breaches

Serious breaches of this policy shall allow the Organisation to terminate your employment with notice. Or terminate your contract with a contractor, agency or temporary worker.

3. Monitoring

3.1 The Organisation reserves the right to monitor communications and access to the Internet, (as applicable) where the communication or is accessed remotely. This includes the use of portable computers and mobile phones issued to the employee by the Organisation.

3.2 The Organisation reserves the monitoring of communications:

Fileserver log file analysis.
Data packet analysis.
Email message analysis, including attachments where required.
Telephone number analysis.

3.3 The Organisation shall assess existing monitoring within the Org assessment will consider the follow

3.3.1 The reason for implementing justified;

3.3.2 The likely adverse impact of communicating with the Organisation

3.3.3 The use of alternatives to monitoring;

3.3.4 Any additional obligations the secure storage of and access to

3.4 The Organisation will also consider such as:

3.4.1 The risk of intrusion into email

3.4.2 The extent to which employees

3.4.3 The impact monitoring will have and the Organisation;

3.4.4 How monitoring will be perceived

3.5 The Organisation shall inform such monitoring or the extension of organisation will inform individual specifically monitored or accessed. where serious breaches of the policy where informing the individual would of data and evidence.

3.6 The Organisation shall take all communications are not accessed. The Organisation can access personal communications that are partly used to pass information. The nature of the personal communications policy.

3.7 The Organisation shall not be responsible for the communications of a personal nature. The organisation or third parties are responsible for the course of their employment.

4. Usernames and Passwords

4.1 You have a duty to keep safe and secure access your PC, portable computer or any device authorised to use by the Organisation.

4.2 For reasons of security you should not attach to or near your PC, portable computer, usernames and or passwords are in your briefcase, carry case or any personal item identifiable as such.

4.3 You should immediately contact *[Insert manager's name]*, to change your usernames and or passwords.

4.4 Where possible and whenever practicable should be made up of a combination of characters. It should consist of names or regular words that are not known to a third party or by software tools used to generate usernames and or passwords.

4.5 If you have any reason to believe your usernames and or passwords have become known to another person not authorised to have access to your information, you should inform *[Insert manager's name]*, immediately. You should also inform how your usernames and or passwords were compromised.

5. Internet Usage

5.1 You have a duty to use the Internet for work-related websites directly related to your work. This includes the company website, (as applicable) and the work-related websites. This duty extends to use of the Organisation's email system.

applicable). You should not at any time access or use any data which promote any of the following:

- i)** sexually explicit materials.
- ii)** violence.
- iii)** discrimination based on race, sex, sexual orientation, or age.
- iv)** illegal activities or violation of applicable laws.
- v)** Furthermore access to streaming services or any other data that uses a large amount of bandwidth is not allowed either during work time or after work time. Such services is directly related to work or business entertainment services such as, "Netflix, Hulu, Amazon Prime, etc."

6. Password Protected Areas

You must not access or attempt to access any password protected areas of the Organisation website, intranet or network. You may access password protected areas of the Organisation partners unless you have been provided with usernames and or passwords by an authorised person. You are not authorised to hold and provide such information to customers or Organisation partners. You are not authorised to provide such information to you.

7. Email Usage Guidelines

7.1 Your email facility within the Organisation must only be used for communication with Organisation partners.

7.2 You should not use your Organisation email facility for personal email messages.

7.3 The Organisation is aware that you may receive non-Organisation partners, friends or associates you may receive email sent. You should instead send an email to the Organisation policy of the Organisation to use your Organisation email facility.

8. Emails are Permanent

It is a common misconception that electronic communication, similar to a phone call, can be traced back to its original source. Copies of emails not only reside on the mobile device of the sender and receiver but also on the Service Provider (ISP) through which they are sent. Even if the chain deletes an email and its attachments, the entire email and attachment can be recovered from PCs and file servers on which they were stored.

9. Proper Deletion of Emails from Email Accounts

9.1 Only emails that breach these policies should be deleted. If you have any queries regarding the deletion of emails, contact the *manager's name* before deleting them.

9.2 To delete a message properly, first delete it from your email software and then delete the message to your bin or trash folder. Do not delete an email from your PC.

10. Email Signature File

All emails, (including replies and forwards), must contain the standard email signature of the Originator. If you are requested to alter or update your email signature, this must be carried out immediately. If you are requested to change your contact information such as office phone number, you should ensure that these details are updated in your signature.

11. Email Etiquette

11.1 You should never send abusive or insulting emails. If you are responding to such an email, do not attack the recipient directly or refer to the sender as an abuser.

11.2 You must never send emails of the following types of content:

- i) sexually explicit materials.
- ii) violence.

iii) discrimination based on race, sex, sexual orientation, or age.

iv) illegal activities or violate intellectual property rights.

11.3 Never send emails containing attachments without first checking that the recipient can receive them via email. Such emails should be easily accessible and readily opened and read by anyone who needs to. If you should contact *[Insert manager's name]* via email, send emails in an encrypted form.

11.4 If you wish to send a large attachment, notify the recipient before sending the email so they can prepare to receive it and that their email and internet connection can download large attachments.

11.5 Do not compose and send email messages that are used to "shout" or exaggerate the volume of your voice. Be rude and offensive.

11.6 Do not attempt to be humorous or sarcastic in emails received by you. Due to the direct nature of email, it is often mistaken for sarcasm or aggression.

11.7 Do not send, resend or forward emails to multiple recipients in the CC field as this will increase the number of recipients and will breach their privacy.

11.8 Do not use ASCII text to create text in your email messages.

12. Third Party Products and Services

You must not use the Internet to download software programs or utilities. Furthermore, you must not copy software from CDs, 3.5 inch diskettes, Zip disks, or any other storage product that you have in your possession, including your mobile device. This also applies to software received from the Organisation. All software received from the Organisation to *[Insert manager's name]* so that it can be distributed to *[Insert manager's name]* with reasonable authority for evaluation and or use.

13. Downloads and Attachments

13.1 You must not download or use utilities on your PC, portable computer or mobile device directly related to your work:

- Mpeg
- MP3
- Peer-to-Peer file sharing services
- Push technology software
- Personalised search software
- Internet Relay Chat software or similar

13.2 Nor any other file format or software that requires video or graphic intensive displays or requires the use of relatively large files to store, distribute or access.

13.3 Furthermore you must not use your mobile device to distribute any of the files listed above within the Organisation or external networks or to receive any of the above from a third party.

14. Transportation and Security

You are reminded, (where provided) that your mobile device may contain confidential and sensitive information and should ensure that your portable computer or mobile device is not left in a vehicle overnight if this can be avoided. If left in the vehicle and if fitted the vehicle should be locked if left unattended. If you cannot see your vehicle, your portable computer or mobile device should not be taken to social events if this cannot be avoided. Your portable computer or mobile device should never leave your portable computer or mobile device out of your direct sight at anytime. Your portable computer or mobile device should always be transported in a secure container within the Organisation.

15. Organisation Access

The Organisation reserves the right to restrict access to its computer or mobile device, (where provided) to those in compliance with these guidelines. Your portable computer or mobile device should be available when required.

16. Faxes

16.1 All faxes should be sent with a cover sheet. All paper copies of faxes should be filed in the administration or client file, complete with the original.

16.2 Never send faxes containing confidential information without first checking that the recipient is authorised to receive it. If the recipient is prepared to receive the fax, it should be sent at a pre-arranged time. You should always send a cover sheet with the fax to inform them of the sender's name and telephone number. After transmission you should check that the fax has arrived and is complete. Do not send routine and confidential or sensitive information by fax, unless the fax number, if available, rather than the telephone number.

17. Telephone Use

17.1 Local and national call-rate payphones should not be used to interfere with your work. Long-distance calls for personal or family nature are not permitted. The exception is for family emergency.

17.2 There are no restrictions placed on the use of telephones for the business of the Organisation is permitted.

17.3 Premium-rate telephone services are not permitted. If such services are used, such calls are for strictly business purposes. Calls for non-business purposes shall cost the user.

17.4 If your telephone has voice-mail, you should ensure it is working correctly, that the message is recorded and that this facility is used by the intended person.

17.5 If you intend to discuss confidential information with another party over the telephone you should ensure that you do not discuss such information. If such information is discussed, ensure that you are not overheard. If how to discuss confidential information with other parties over a speaker or conference call, the confidential conversation should be identified and the confidentiality of the information maintained.

17.6 All conference calls, (regardless of whether confidential information is discussed) should take place in a secure environment where discussion cannot be overheard from other parties.

conference call should be identified
conversation leaves or a new party
participants.

18. Mobile Phone Use

You are reminded that personal vo
mobile phone (if supplied by the O
The Organisation reserves the righ
the Organisation to ensure complia

19. Authority

You must not use any form of com
represent that you have the autho
or use any form of communication
Organisation.

20. Date of Implementation

This policy is effective from *[Insert*
that occurred prior to this date.

21. Questions

If you have any questions regardin
you, please consult *[Insert manag*

22. Alteration of this Policy

This policy will be subject to chang
communicated to you by *[Insert m*

EXAMPLE DOCUMENT

COMMUNICATIONS POLICY

This policy document regarding Internet usage is part of the terms and conditions of your contract with **Digital Partners**, ("the Organisation").

This policy applies to your employment with the Organisation and all other Organisation sites that you access at any time. This policy must also be observed at all partner facilities. Employees must adhere to any communication guidelines exist at client or partner sites.

Please note that this policy also applies to any contractor, agency worker, temporary staff or other Organisation.

For any policy to be effective it must be understood and apply to all staff regardless of location.

If you have any questions regarding this policy you please consult **Peter J Thompson** or any other staff that may breach these guidelines.

1. Minor Breaches

Minor breaches of this policy shall be dealt with using the disciplinary procedure.

2. Serious Breaches

Serious breaches of this policy shall allow the Organisation to terminate your contract with notice. Or terminate your contract with a contractor, agency or temporary worker.

3. Monitoring

3.1 The Organisation reserves the right to monitor communications and access to the Internet, (as applicable) where the communication or is accessed remotely.

includes the use of portable computers and mobile phones issued to the employee by the Organisation.

3.2 The Organisation reserves the right to monitor the monitoring of communications:

Fileserver log file analysis.

Data packet analysis.

Email message analysis, including attachments where required.

Telephone number analysis.

3.3 The Organisation shall assess the impact of any existing monitoring within the Organisation. The assessment will consider the following:

3.3.1 The reason for implementing monitoring is justified;

3.3.2 The likely adverse impact on the privacy of employees communicating with the Organisation;

3.3.3 The use of alternatives to monitoring;

3.3.4 Any additional obligations that may arise from the secure storage of and access to data.

3.4 The Organisation will also consider the following:

3.4.1 The risk of intrusion into employee data;

3.4.2 The extent to which employees are aware of monitoring;

3.4.3 The impact monitoring will have on the privacy of employees and the Organisation;

3.4.4 How monitoring will be perceived by employees.

3.5 The Organisation shall inform employees of any such monitoring or the extension of monitoring. The Organisation will inform individual employees if they are specifically monitored or accessed. The Organisation will inform employees where serious breaches of the policy occur and where informing the individual would be in the best interests of data and evidence.

3.6 The Organisation shall take all communications are not accessed. The Organisation can access personal communications that are partly used to pass information of the nature of the personal communications policy.

3.7 The Organisation shall not be responsible for the communications of a personal nature of the organisation or third parties at the course of their employment.

4. Usernames and Passwords

4.1 You have a duty to keep safe and secure any system or device that is authorised to use by the Organisation.

4.2 For reasons of security you should not store usernames and or passwords in a briefcase, carry case or any personal item identifiable as such.

4.3 You should immediately contact **Peter J Thompson** to change your username and or password.

4.4 Where possible and whenever practicable passwords should be made up of a combination of letters, numbers and symbols. Passwords should consist of names or regular words that are not known to a third party or by software tools used to generate usernames and or passwords.

4.5 If you have any reason to believe that your usernames and or passwords have become known to another person who is not authorised to have access to your information you should inform **Peter J Thompson** immediately. You should also change your usernames and or passwords.

5. Internet Usage

5.1 You have a duty to use the Internet for work related purposes. You should not visit websites directly related to your work or the Organisation website, (as applicable) and the work of the Organisation.

This duty extends to use of the Or (applicable). You should not at any which promote any of the following

- i)** sexually explicit materials.
- ii)** violence.
- iii)** discrimination based on race, s orientation, or age.
- iv)** illegal activities or violation of
- v)** Furthermore access to streamer any other data that uses a large a not allowed either during work tim such services is directly related to entertainment services such as, "r

6. Password Protected Areas

You must not access or attempt to Organisation website, intranet or r Organisation partners unless you h usernames and or passwords by a authorised to hold and provide suc customers or Organisation partner to provide such information to you

7. Email Usage Guidelines

7.1 Your email facility within the O must only be used for communicat

7.2 You should not use your Organ personal email messages.

7.3 The Organisation is aware that policy in place. If you receive non-partners, friends or associates you sent. You should instead send an e policy of the Organisation to use y

8. Emails are Permanent

It is a common misconception that electronic communication, similar to a phone call, can be traced back to its original source. Copies of emails not only reside on the mobile device of the sender and recipient but also on the Service Provider (ISP) through which they are sent. Even if the chain deletes an email and its attachments, the entire email and attachment can be recovered from PCs and file servers on which they were stored.

9. Proper Deletion of Emails from Email Accounts

9.1 Only emails that breach these policies should be deleted. In response to any queries regarding the deletion of emails, contact **Thompson** before deleting the email.

9.2 To delete a message properly, first delete it from your email software and then delete the message to your bin or trash folder. Do not delete an email from your PC.

10. Email Signature File

All emails, (including replies and forwards) must contain the standard email signature of the Originator. Any request to alter or update your email signature must be carried out immediately. If you have any changes to your contact information such as office phone number, you should ensure that these details are updated in your signature.

11. Email Etiquette

11.1 You should never send abusive or harassing emails. If you are responding to such an email, do not attack the recipient directly or refer to the sender as abusive or harassing.

11.2 You must never send emails containing the following types of content:

- i)** sexually explicit materials.
- ii)** violence.

iii) discrimination based on race, sex, sexual orientation, or age.

iv) illegal activities or violate intellectual property rights.

11.3 Never send emails containing sensitive information without first checking that the recipient is intended to receive it via email. Such emails should be encrypted and should not be readily opened and read by anyone other than the intended recipient. If you should contact **Peter J Thompson** via email, please use an encrypted form.

11.4 If you wish to send a large attachment, please notify the recipient before sending the email so they can prepare to receive it and that their email and internet connection can download large attachments.

11.5 Do not compose and send email messages that are used to "shout" or exaggerate the volume of your voice. Do not be rude and offensive.

11.6 Do not attempt to be humorous or sarcastic in emails received by you. Due to the direct nature of email, humor is often mistaken for sarcasm or aggression.

11.7 Do not send, resend or forward sensitive information to recipients in the CC field as this will notify all recipients and will breach their privacy.

11.8 Do not use ASCII text to create sensitive information in your email messages.

12. Third Party Products and Services

You must not use the Internet to download software, programs or utilities. Furthermore, you must not copy software from CDs, 3.5 inch diskettes, Zip disks, or any other storage product that you have in your possession, or from any mobile device. This also applies to software received from the Organisation. All software received from the Organisation to **Peter J Thompson** so that it can be reviewed by **Peter J Thompson** with reasons for approval, rejection, evaluation and or use.

13. Downloads and Attachments

13.1 You must not download or use utilities on your PC, portable computer or mobile device directly related to your work:

- Mpeg
- MP3
- Peer-to-Peer file sharing services
- Push technology software
- Personalised search software
- Internet Relay Chat software or similar

13.2 Nor any other file format or software that requires video or graphic intensive displays or requires the use of relatively large files to store, distribute or access.

13.3 Furthermore you must not use your mobile device to distribute any of the files listed above within the Organisation or external networks or to receive any of the above from a third party.

14. Transportation and Security

You are reminded, (where provided) that your mobile device may contain confidential and sensitive information and should ensure that your portable computer or mobile device is not left in a vehicle overnight if this can be avoided. If left in the vehicle and if fitted the vehicle should be locked if left unattended. If you cannot see your vehicle, your portable computer or mobile device should also be locked if you cannot see your vehicle. Your portable computer or mobile device should never leave your portable computer or mobile device of your direct sight at anytime. Your portable computer or mobile device should always be transported in a secure container within the Organisation.

15. Organisation Access

The Organisation reserves the right to access your portable computer or mobile device, (where provided) to ensure compliance with these guidelines. Your portable computer or mobile device should always be available when required.

16. Faxes

16.1 All faxes should be sent with a cover sheet. All paper copies of faxes should be filed in the administration or client file, complete with the original.

16.2 Never send faxes containing confidential information without first checking that the recipient is authorised to receive it. If the recipient is prepared to receive the fax, it should be sent at a pre-arranged time. You should always call the recipient before sending the fax to inform them of the time and date of the fax number. After transmission you should call the recipient to confirm that the fax has arrived and is complete. Faxes should not be sent via a routine and confidential or sensitive information. Always use the fax number, if available, rather than the telephone number.

17. Telephone Use

17.1 Local and national call-rate payphones should not be used to interfere with your work. Long-distance calls for personal or family nature are not permitted. The exception is for family emergency.

17.2 There are no restrictions placed on the use of telephones for the business of the Organisation is permitted.

17.3 Premium-rate telephone services are not permitted. If such services are used, they must be for strictly business purposes. Calls for non-business purposes shall cost the user.

17.4 If your telephone has voice-mail, you should ensure it is working correctly, that the message is recorded and that this facility is used by the intended person.

17.5 If you intend to discuss confidential information with another party over the telephone you should ensure that you do not discuss such information. If such information is discussed, ensure that you are not overheard. If how to discuss confidential information with other parties over a speaker or conference call, the confidential conversation should be identified and the confidentiality of the information maintained.

17.6 All conference calls, (regardless of whether confidential information is discussed) should take place in a secure environment where discussion cannot be overheard from other parties.

conference call should be identified
conversation leaves or a new party
participants.

18. Mobile Phone Use

You are reminded that personal vo
mobile phone (if supplied by the O
The Organisation reserves the righ
the Organisation to ensure complia

19. Authority

You must not use any form of com
represent that you have the autho
or use any form of communication
Organisation.

20. Date of Implementation

This policy is effective from **8th No**
actions that occurred prior to this

21. Questions

If you have any questions regardin
you, please consult **Peter J Thom**

22. Alteration of this Policy

This policy will be subject to chang
communicated to you by **Peter J T**