Social Media, internet, intranet and e-mail Policy

Overview

Who the policy affects

The policy applies to all members or representatives of the organisation.

Purpose

This policy supports employees and representatives of Dewi Development Ltd make decisions on the best use of internet media and communication in their work, while ensuring they represent the organisation in an appropriate and legal manner.

Dewi Development Ltd encourages employees and representatives to use internet media and communication to effectively carry out their work and to promote the organisation.

This policy highlights that employees and representatives must ensure they do not breach intellectual property, breach confidentiality, transfer restricted documentation or bring the organisation into disrupt.

Scope

The policy includes all people representing the organisation from director to employee, temporary staff, sessional staff, agency staff, contractors and volunteers. All employees are included whether full time, part time, office based or home worker.

The policy includes e-mail, intranet, internet, instant messaging and social media. This includes media, but limited to, text, pictures, video, audio and blogging. These may be on, but not limited to, Facebook, Twitter, Snapchat, Instagram, LinkedIn, Google+, Flickr, WhatsApp, Pin Interest and Wikipedia.

The policy applies to people using work computer systems, corporate social media profiles and personal computer systems or person social media profiles where Dewi Development Ltd is represented within the information shared.

The policy does not form part of the terms and conditions of employment with Dewi Development Ltd.

Effective Date

This policy applies from the 29 January 2019.

The company holds to right to update the policy at any time.

Policy

1. General communication

1.1. Do not share any media or write any text that may embarrass or bring into distribute Dewi Development Ltd.

1.2. Do not communicate anything that you know is untrue.

1.3. Do not download or share any media that may:

- 1.3.1. Encourage or promote activities that are illegal or unlawful
- 1.3.2. May be considered to be indecent, obscene or contain profanity
- 1.3.3. May be considered as offensive, abusive, a personal attack, threatening or racist
- 1.3.4. May be inflammatory or incur liability of Dewi Development Ltd
- 1.3.5. May cause overload of our systems

1.4. When communicating, do not commit Dewi Development Ltd to any action unless you have the authority to do so.

1.5. Respect all intellectual property and copyright and do not share any content Dewi Development does not have rights to.

1.6. Be aware the written communication can be misconstrued and that there is limited tone to written communication. It may be better and quicker to make a phone call than use written communication.

1.7. Be aware that written communication on business time or regarding business activity is the property of the business and may be used as evidence of communication. Where evidence of communication is required, written communication would be better than a conversation.

1.8. The use of personal communication media may take place in your own personal time where it is in keeping with guidance of this policy. Your own personal time is outside of working hours, during lunch or on a break.

2. Voice and video conversation

2.1. Do not leave voice mails for individuals containing protected or confidential information, as you do not know if the voicemail records silently or who can pick up the voice message. This includes any data that would be classed as personal under GDPR.

2.2. When undertaking protected or confidential conversations, ensure you are in appropriate area where people cannot listen into the conversation and that the individual receiving the call is somewhere confidential.

2.3. When undertaking video calls containing protected or confidential information, ensure people cannot see through windows to see the information on the screen or that they could see the speaker and lip read.

2.4. When undertaking video calls ensure that no information on the desk or walls can be seen in the call that is protected or confidential.

3. E-mail

3.1. Corporate e-mails may not be forwarded to personal e-mail accounts or forwarding rules set up to do so.

3.2. Forwarding rules may not be setup to other individuals accounts. If employee is on leave or leaves the organisation, appropriate proxy to accounts should be defined to appropriately authorised level of staff.
3.3. Attachments containing confidential information should not be shared by e-mail, but shared through the corporate FTP site where access can be managed.
3.4. Before opening any file, ensure you know who the sender is, that the sender address has not been phished and you recognise the file format.
3.5. Do not open any files that are executables (.exe) without first discussing with IT.
3.6. Large files should not be shared over e-mail, with a maximum limit of 20MB.
3.7. You may access personal e-mails in your own time, as long e-mail content is in keeping with the same standards as business e-mails and opening will not cause offence to any colleagues around you.

4. Instant messaging

4.1. Corporate messages may not be forward to personal instant message accounts. The exception is marketing messages that the sender can forward to promote the organisations.
4.2. An attachment containing confidential information should not be shared by instant messaging. A link to the corporate FTP site can be shared where the access to the file can be managed.
4.3. Before opening any file, ensure you know who the sender and you recognise the file format.
4.4. Where the app informs you that the security code has been changed and you are not aware the recipient has changed their phone or app, check with the individual before exchanging further information.

5. Social media

5.1. Do not share any corporately sensitive, anti-competitive or confidential information.
5.2. Do not forward or post any content that may be seen as derogatory, incentive, discriminatory, offensive, illegal or unlawful.
5.3. Do not forward, share or comment on any content from the corporate account which is not in keeping with the ethos of Dewi Development Ltd and could suggest that Dewi Development Ltd is endorsing or affiliating with the content.
5.4. Be mindful of how posts on social media can be perceived and how employees' responses to customers posts can represent Dewi Development Ltd.
5.5. When on sites like LinkedIn you may not provide professional references, unless it is part of your job role. You may provide personal references as long as it clearly states it is personal reference.
5.6. When commenting on social media, be transparent that these are your thoughts and not the thoughts of Dewi Development Ltd.
5.7. You may access your personal social media accounts in your own time, as long social media content is in keeping with the same standards as business e-mails and opening will not cause offence to any colleagues around you.

6. Internet

6.1. You may view non-business related sites but are responsible for what you view.

6.2. You should not view any sites that holds sexually explicit information or provides information on carrying out an activity that is illegal or unlawful.
6.3. You should not download any files where you are not sure of the provider, the content or of the file type.
6.4. When viewing sites that are transferring information, for example personal data or bank details ensure that the site uses SSL encryption and the encryption is enforce with green padlock in the address bar.
6.5. Always check the path of internet address is as expected and not phising site with slightly different address.
6.6. You may view the internet for personal use in your own time, as long as content viewed is in keeping with the same standards as business viewing.

7. Access work from home

7.1. You may access work information from home where:
- 7.1.1. Your network is appropriately secured
- 7.1.2. Your electronic device is appropriately secured with user credentials
- 7.1.3. You have appropriate virus and anti-malware software installed and active

7.2. You may not download company documents that have a confidentiality level of 'Protected' or above to your home machine.

8. Passwords

8.1. Passwords should not be shared, and group passwords should not be set up.
8.2. If a password is asked for by IT, the passwords should not be provided. IT will not ask for this information.
8.3. New passwords set up by IT, should be changed by individual on first log in.
8.4. If passwords need to be written down in case they are forgotten, they should be stored securely in a safe that is only accessible to that individual.
8.5. Passwords stored electronically should be stored in encrypted file, ideally a cooperate Password Locker.
8.6. Passwords must not be written down and left anywhere, for example on post-it note on the screen, on the desk or in the draw.

9. Document security

9.1. When not at your desk:
- 9.1.1. Protected or confidential documents must not be left on display on a computer screen
- 9.1.2. The computer should be locked by user or if away for long periods of time, the computer should be logged out
- 9.1.3. Protected or confidential documents printed documents must not be left on the desk, but stored in secure cabinets.

10. Prohibited activities

10.1. You should not carry out the following activities within the premises of Dewi Development Ltd or on any device belonging to Dewi Development Ltd.
- 10.1.1. Knowingly attempting to access data you know or should know is confidential and therefore is unauthorised access

10.1.2. Carrying out hacking activity
10.1.3. Accessing or attempting to access restricted areas of the network
10.1.4. Introduction of any virus or malware
10.1.5. Introducing network monitoring software, password detecting software or key loggers on to the network
10.1.6. Installing software not agree with IT department
10.1.7. Storing personal data on Dewi Development Ltd network
10.1.8. Requesting another individual's login credentials and passwords
10.1.9. Sharing your login credentials or passwords

11. Security breaches

11.1. Where it is believed that an account, username or password has become unsecure, the security for the account should be changed immediately.

11.2. Breaches should be reported to the Chief Information Officer, to decide if a report must take place under GDPR regulations. This must happen within 72 hours.

12. Monitoring

12.1. The use of the internet, social media and emails are subject to monitoring, including personal use which is carried out on Dewi Development Ltd premises or hardware.

12.2. Where monitoring identifies that breaches of the policy has occurred, action may be taken.

12.3. Dewi Development Ltd reserves the right to restrict access to any sites, e-mail address or domains.

12.4. Dewi Development Ltd may review employees, contractors or volunteers' social media accounts, to check Dewi Development Ltd is not being misrepresented or brought in disrepute or that employee is not in keeping with this policy. If a review identifies a breach of policy has occurred, action may be taken.

Compliance

The non-compliance with this policy may lead to disciplinary action or possible dismissal in line with the laws of the employing country.

Definitions

Media refers to text, blog, post, pictures, audio and video.

Document Information

Document Control

Document Confidentiality	General Audiences
Confidentiality Classification	Internal
Document Owner	Information Officer
Approved By	David Husband
Approval Date	29/01/2019
First Published	29/01/2019
Review Date	01/02/2021
Related documents	Document Management Procedure
Status	Published

Version

Version	Author	Date	Summary Changes
0.1	David Husband	26/01/2019	
1.0	David Husband	29/01/2019	Approval
2.0	David Husband	20/05/2019	Security Breaches Document Security Voice and Video conversations

Authors

Author	Company	Job Title	Department
David Husband	Dewi Development	Director	Management

Retention

Retention date	N/A
Retention details	Document is appropriate until replaced.

Disposal

Disposal classification	Not Controlled
Disposal details	Document does not contain commercially sensitive information. Paper copies should be recycled.