Digital Communication Policies and Procedures

[COM001]

Contents

1. Purpose 2

2. Policies and Procedures 2

2.1 Request for Software 2

2.2 Purchase of Software 2

2.3 Obtaining Open Source or Freeware Software 3

2.4 Implementing New and Emerging Technologies 3

2.5 Commonly Used Digital Communication Tools 3

2.6 Professional Communication Etiquette 4

2.6.1 Email Etiquette 4

2.6.2 Social Media Etiquette 5

2.7 Digital Data Security 6

1. Purpose

This policy provides guidelines around digital communication at Bounce Fitness, including for the purchase of software for the business and its appropriate use by all staff.

The aim of this policy is to ensure that digital tools and software introduced to and used by Bounce Fitness and its staff are appropriate, value for money and where applicable integrates with other technology for the business. This applies to software obtained as part of hardware bundle or pre-loaded software.

Bounce Fitness is committed to provide the necessary training for all staff to ensure they use the selected digital tools and software appropriately, in a professional way, aligning with the company's values and philosophy.

The policies and procedures outlined below must be adhered to when implementing new and emerging digital technologies into the business operations

2. Policies and Procedures

2.1 Request for Software

All software, such as open source, freeware, etc. must be approved by the Information Technology Manager prior to the use or download of such software.

2.2 Purchase of Software

The purchase of all software must adhere to this policy.

All purchased software must be purchased by the Information Technology Manager.

All purchased software must be purchased from authorized distributors.

All purchases of software must be supported by appropriate warranty provided by the distributor and be compatible with the business's server and/or hardware system.

Any changes from the above requirements must be authorised by the Information Technology Manager.

All purchases for software must be in line with the purchasing policy in the *Financial Policies and Procedures* manual.

2.3 Obtaining Open Source or Freeware Software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from Information Technology Manager must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the business's hardware and software systems.

Any change from the above requirements must be authorised by Information Technology Manager.

2.4 Implementing New and Emerging Technologies

When the need for using new and emerging technologies arises, relevant policies and procedures must be followed for requesting and purchasing/obtaining the software.

Once approval is obtained as outlined above, branch manager must inform relevant staff about the new technology and a training must be organized for using the software. Branch managers must send out an email communication to all clients and relevant stakeholders a minimum of one week prior launching the technology to inform them about the change and to explain how this may affect them.

Three months after implementing the new technology, a survey must be sent out to all clients and relevant stakeholders to seek feedback.

2.5 Commonly Used Digital Communication Tools

Bounce Fitness employees and personnel must use the following to send digital communication relevant to the workplace:

- Gmail
  - Used for sending work-related emails and reminders
  - Used for sending confidential information among staff members
- Slack
  - Used for instant messaging among staff members
- Skype
  - Used for phone and video conferencing

  - Used for sending commercially sensitive client information to staff members using the Private Conversation feature

2.6 Professional Communication Etiquette

Bounce Fitness ensures that all staff members follow professional communication etiquette, even when using digital communication. These include:

- Include proper greetings at the start of each email
- Follow proper grammar and correct sentence structures
- Use polite language in all communication
- Avoid discussing personal matters with clients
- Limit the use of emojis

At Bounce Fitness, all staff members follow professional communication etiquette, even when using digital communication. These include:

- Including proper greetings at the start of each email
- Follow proper grammar and correct sentence structures
- Using polite language in all communication
- Avoiding discussing personal matters with clients
- Limiting the use of emojis
- Not making excuses or blaming others when mistakes are made

2.6.1 Email Etiquette

All outgoing emails and formal emails must:

- Always have text in the email body (do not send blank emails or emails with pictures only)
- Employ correct grammar, spelling, and punctuation
- Use formal English (avoid using slang and emojis)
- Use appropriate font (e.g. Arial, Calibri, Cambria, Garamond, Trebuchet)
- Avoid using too many colours and highlights in the email
- Use one dark colour in the main email body (preferred colours are black, dark grey, or navy blue)

- The intended audience of the email must be clearly identified [e.g. “Hi, Mark.” Or “To all fitness instructors:”
- The purpose of the email must be clearly indicated [e.g. “To clarify your discussion this morning…”]
- Regardless of the intended audience [client, suppliers, colleagues, etc.], violent, pornographic, or otherwise inappropriate content in the emails is strictly not allowed.
- All emails with attachments must have a clear description of the attachment in the main body text of the email [e.g. “Hi John. Here is the e-book that I told you about last Friday”].
- Suspicious emails with attachments must be received with caution. The receiver of the email may confirm or ask for information about the attachment from the sender. The attachment must NOT be opened until there is enough evidence that the attachment is safe.
- Urgent emails must be marked as ‘high importance.’
- All urgent emails received must be addressed immediately.
- All potentially dangerous emails must be deleted immediately.
- Do not open emails from suspicious senders.

2.6.2 Social Media Etiquette

- All staff members communicating with clients or potential clients through the Official Facebook Page must still use proper English.
- Proper grammar, spelling, and punctuation must still be used, though it may be more casual.
- Some emojis may be used, but this must be used sparingly.
- Slang may be used, but sparingly.
- Violent, aggressive, or otherwise inappropriate language must not be used.
- All spam messages on Facebook pages must be deleted. Do not respond.
- Internet “trolls” must be ignored. Do not respond. These accounts may be reported, if necessary.

2.7 Digital Data Security

Moreover, Bounce Fitness aims to continuously ensure the security of digital data within the workplace. In order to meet this, Bounce Fitness uses secure platforms that provide encryption for workplace tasks. The following etiquette is observed:

- Using only official Bounce Fitness-prescribed platforms when communicating about work-related matters, such as the following:
    - Report checking
    - Scheduling of events and meetings
    - Document feedback

This is conducted between the following Managers, who create the reports for submission, and the Chief Executive Officer, who is the report recipient:

- General Manager Finance
- General Manager Human Resource
- General Manager Marketing

Do not open suspicious communication – do not open files or click on links – even if the sender is supposedly a Bounce Fitness employee.

Based on industry etiquette, staff members at Bounce Fitness follow these practices:

- Using digital communication applications with encryption when communicating with work colleagues
    - This ensures access to files transferred and messages will be limited to the sender and the recipient.
    - This protects information from cyber-attacks.
- Using workplace email account:
    - Email sent using your work account is only limited to work-related email.
    - Passwords should be changed every six months.

Date	Summary of Modifications	Version
3 August 2021	Policy and procedure document approved by Vijay Thor	1.0
27 September 2021	Removed repeated text in the Policies section	1.1

11 March 2022	Included the implementation of new and emerging technologies	2.0