Bhutan Standard Bureau

ICT Acceptable Usage Policy (AUP) for BSB staff.

1. Introduction

As use of the internet by staff becomes more widespread, for the protection of the organization, the staff and volunteers it is necessary to set out some guidelines for internet use. Staff should read these guidelines carefully, in conjunction with the organization ICT Security Policy. Abuse of the internet may lead to disciplinary action being taken.

The use of electronic communication and information retrieval is no more than the addition of another medium. **The same behavioural and professional standards are expected of staff as are the case with traditional written communications, the telephone and face to face meetings.**

The internet as a resource is constantly changing. These guidelines will be updated in the light of experience and developments of the internet itself.

Please Note: The following acceptable use policy refers to ICT use for staff in BSB - this would need to be adapted dependent on the setting and how and when staff have access to the internet.

2. Acceptable Uses

As a general principle, internet access is provided to staff to support work related activities. The following list is not intended to be a definitive list, but sets out broad areas of use that the organization considers to be acceptable uses of the internet:

- To provide communication within the organization via email or the organization website
- To provide communication with other organizations for educational purposes
- To distribute electronic copies of the weekly bulletin and newsflash
- To distribute details regarding organization meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions.

3. Unacceptable Uses

The following uses will be regarded as not acceptable:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy Use for racial, sexual, homophobic or other harassment.
- To access pornographic, obscene or illegal material.
- To solicit personal information with the intent of using such information to cause harm.
- Entering into a commitment on behalf of the organization (unless you have explicit permission to do this).
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Publishing defamatory and/or knowingly false material about the organization, your colleagues and/or our young people on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.

- Revealing confidential information about the organization in a personal online posting, upload or transmission - including financial information and information relating to our young people, staff and/or internal discussions.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network.
- To disrupt the work of other users. This includes the propagation of computer viruses and use of the internet.
- Use for personal or private business purposes.

4. Netiquette

The following general principles should be adopted:

- Be polite. Do not be abusive in messages to others.
- Use appropriate language.
- Remember that you are a representative of the organization and that you are using a non-private network.

5. Email

Whenever e-mail is sent, it should be from an official work email address which includes the sender's name, job title and organization's name.

- Every user is responsible for all mail originating from their user ID (e-mail address).
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
- Attempts to send junk mail and chain letters are prohibited.
- If you receive e-mail from outside the organization that you consider to be offensive or harassing, speak to your line manager (harassing internal e-mail will be dealt with under the organization's guidelines).
- You should be aware that, in the event of the organization being involved in legal proceedings, any relevant e-mails (including internal e-mail) may have to be disclosed, on the same basis as is the case for written documents.
- Email should be accessed via organization ICT equipment only, if you wish to use a personal device to download organization emails, you must check with your line manager first.
- You will need to ensure that your device is secured by a password at all times, that this password is not shared with any other person and that all reasonable care is taken to prevent unauthorised access to confidential information.

6. Social Networking Sites

Social media applies to blogs, microblogs like Facebook, Twitter, LinkedIn, videos, social networks, discussion forums, wikis, and other personal webspace. This organization permits the use of internet and social media on work premises, outside of work time, but only where it meets the following guidelines. This is usually outside

normal working hours and must not interfere with your or others day-to-day duties. Personal access should not be in view of any young people, and you are reminded to log out or 'lock' the screen immediately upon leaving your mobile phone or PC, even if only for a short while.

- Do not "speak" for the organization unless you have express permission to do so, this covers all comments relating to the organization.
- Protect yourself from identity theft
- If you can be linked to the organization, act appropriately. This includes photos and status updates
- Remember that colleagues, prospective employers, parents and children may see your online information
- The organization policy is that you are not allowed to be 'friends' with young people with whom you work or have worked with in the past unless there are exceptional circumstances, e.g. child, sibling etc Please choose your 'friends' carefully, especially in light of the last above.
- Ensure your settings are on private and only you and YOUR friends can see them.
- If in doubt, please seek advice in organization.

7. Disciplinary Action

Disciplinary action may be taken against staff and volunteers who contravene these guidelines, in accordance with the organization's disciplinary procedures.

8. Advice

If you require any advice on the use of these guidelines, please contact ICT, BSB.

I have read and agree to abide by the rules stated in the I.C.T. Acceptable Usage Policy. I understand the consequences if I do not.