Internet & Email Usage

2015 hUMAN rESOURCES tOOL kIT

DEVELOPED BY APEX HUMAN RESOURCES FOR THE DEPARTMENT OF SPORT AND RECREATION

**Internet and Email Usage Policy and Guidelines**

Introduction

This policy sets out the obligations and expectations on employees of the organisation including contractors and temporary staff, who use the organisation’s IT facilities for internet and email purposes. IT facilities are provided to assist with day to day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal professional and ethical obligations that apply to them.

Authorisation

No person is allowed to use Organisation IT facilities who has not previously been authorised to do so by the Organisation IT Department / Line Manager. Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

Legislation

All users shall comply with the relevant legislation regarding data protection.

Users need to be sure that they are not breaching any data protection when they write and send emails. This could include but is not limited to:

* Passing on personal information about an individual or third party without their consent.
* Keeping personal information longer than necessary.

Email should where possible be avoided when transmitting personal data about a third party.This includes comment and opinion, as well as factual information. Therefore this should be borne in mind when writing emails, and when keeping them.

Responsibilities

All Users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services. Any accidental damage or disruption must be reported to IT / Line Manager as soon as possible after the incident has occurred. Users are responsible for any IT activity which is initiated under their username.

**Use of the Internet**

Use of the Internet by employees is encouraged where such use is consistent with their work and with the goals and objectives of the organisation in mind. Reasonable personal use is permissible subject to the following:

* Users must not participate in any online activities that are likely to bring the organisation into disrepute, create or transmit material that might be defamatory or incur liability on the part of the organisation, or adversely impact on the image of the organisation.
* Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs.
* Users must not knowingly introduce any form of computer virus into the organisation’s computer network.
* Personal use of the internet must not cause an increase for significant resource demand, e.g. storage, capacity, speed or degrade system performance.
* Users must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such licence.
* Users must not use the internet for personal financial gain.
* Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
* Users must not use the internet to send offensive or harassing material to other users.
* Use of the internet for personal reasons (e.g. online banking, shopping, information surfing) must be limited, reasonable and done only during non-work time such as lunch-time.
* Use of gambling sites, online auction sites and social networking sites such as, but not limited to, Facebook, LinkedIn, Youtube, Twitter, Bebo, Flickr, MySpace etc is **not** permissible.
* Staff may face disciplinary action or other sanctions (see below) if they breach this policy and/or bring embarrassment on the Organisation or bring it into disrepute.

**Use of Email**

Emails sent or received on the email system form part of the official records of the organisation; they are not private property. The organisation does not recognise any right of employees to impose restrictions on disclosure of emails within the organisation. Users are responsible for all actions relating to their email account/pc username and should therefore make every effort to ensure no other person has access to their account.

When using organisation email, users must:

* ensure they do not disrupt the organisation’s wider IT systems or cause an increase for significant resource demand in storage, capacity, speed or system performance e.g. by sending large attachment to a large number of internal recipients, without receiving prior authorisation
* ensure they do not harm the organisation’s reputation, bring it into disrepute, incur liability on the part of the organisation, or adversely impact on its image.
* not seek to gain access to restricted areas of the network or other “hacking activities” is strictly forbidden
* must not use email for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Employees who receive emails with this content from other employees of the organisation should report the matter to their line manager or supervisor.
* not send email messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libellous or contain illegal or offensive material, or foul language.
* not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
* not engage in any activity that is likely to
  + - Corrupt or destroy other users’ data or disrupt the work of other users
    - Waste staff effort or organisation resources, or engage in activities that serve to deny service to other users
    - Be outside of the scope of normal work-related duties – for example, unauthorised selling/advertising of goods and services
    - Affect or have the potential to affect the performance of damage or overload the organisation system, network, and/or external communications in any way
    - Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights
* not send chain letters or joke emails from an organisation account.

Staff who receive improper email from individuals inside or outside the organisation, should discuss the matter in the first instance with their line manager or supervisor.

Good Practice

The organisation has good practice guidelines for dealing with email when staff are out of the office for longer than three days. When activating the "out of office" facility messages should name an alternative member of staff for correspondents to contact if necessary. This will ensure that any important messages are picked up and dealt with within required timescales.

During periods of absence when highly important emails are anticipated, the employee (or manager) should make arrangements for notification and access by another appropriate member of staff.

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender’s knowledge. They may be read by persons other than those they are intended for.

Users must exercise due care when writing emails to avoid being rude or unnecessarily terse. Emails sent from the organisation may be interpreted by others as organisation statements. Users are responsible for ensuring that their content and tone is appropriate. Emails often need to be as formal and businesslike as other forms of written correspondence.

Users should delete all personal emails and attachments when they have been read and should also delete all unsolicited junk mail. In the process of archiving emails, users should ensure inappropriate material is not archived

(Organisation) provides a current and up to date automatic virus checker on all networked computers. However, caution should be used when opening any attachments or emails from unknown senders. Users must best endeavour to ensure that any file downloaded from the internet is done so from a reliable source. It is a disciplinary offence to disable the virus checker. Any concerns about external emails, including files containing attachments, should be discussed with the IT / Line Manager.

**Remote Users**

Employees may sometimes need to use organisation equipment and access the organisation network while working remotely, whether from home or while travelling. The standards set out in this document apply whether or not organisation equipment and resources are being used.

**Penalties for Improper Use**

Breaches of these regulations may be dealt with under the Organisation’s disciplinary procedures. It may lead to termination of employment from the Organisation.

Where appropriate, breaches of the law will be reported to the police.

**Social Media Policy**

Social media offers the opportunity for people to gather in online communities of shared interest and create, share or consume content. As a member based organisation, (Organisation name) recognises the benefits of social media as an important tool of engagement and enrichment for our stakeholders. It is important that the reputation of (Organisation name) and the sport generally is not tarnished by anyone using social media tools inappropriately, particularly in relation to any content that might reference the organisation.

When someone clearly identifies their association with (Organisation name), and/or discusses their involvement in the organisation in this type of forum, they are expected to behave and express themselves appropriately and in the ways that are consistent with (Organisation Name) stated values and policies.

This policy aims to provide some guiding principles to follow when using social media. This policy does not apply to the personal use of social media platforms by members or staff that makes no reference to (Organisation Name) or related issues.

**Scope**

This policy applies to (Organisation Name) members, member clubs, officials, staff and any other formal representatives of the organisation.

This policy covers all forms of social media. Social media includes, but is not limited to, activities such as:

* Maintaining a profile page on social or business networking sites (such as LinkedIn, Facebook, Twitter or MySpace);
* Content sharing including Flicker (photo sharing) and YouTube (Video Sharing);
* Commenting on blogs for personal or business reasons;
* Leaving product or service reviews on retailer sites or customer review sites;
* Taking part in online votes and polls;
* Taking part in conversations on public and private web forums (message boards)

The intent of this policy is to include anything posted online where information is shared that might affect members, colleagues, sponsors or (Organisation Name) and the reputation of the sport in general.

**Guidelines**

For (Organisation name) members, officers and staff using social media, such use:

* Must not contain, or link to, libellous, defamatory or harassing content;
* Must not comment on, or publish information that is confidential in anyway
* Must not bring the organisation or the sport into disrepute.
* Under no circumstance should offensive comments be made about the sports members, volunteers or staff online.

**Breach of Policy**

If detected or reported a breach of this policy may result in disciplinary action being taken.

A breach of this policy may also amount to breaches of other (Organisation Name) policies. This may involve a verbal or written warning or in serious cases, termination of employment or engagement with (Organisation Name) including suspension of membership.