WEIGHTLIFTING WALES
CODI PWYSAU CYMRU

Information and Communication Technology Policy and Procedures

Approved: October 2016

Review: October 2019

Information and Communication Technology (ICT) Information Policy and Procedure

Policy, standards, guidelines and procedures have been established to ensure that (ICT) facilities, services, programs and data are protected from all threats, whether internal or external, deliberate or accidental.

All Users (i.e. anyone with access) is covered by this policy and related procedures.

ICT Acceptable Use Policy

All users who are granted access to, or use WW Information and (ICT) facilities or services shall use them in an appropriate and responsible manner that further the aims of our sport. Disciplinary actions apply, for violation of this policy and/or procedures.

1. Objectives of the Policy

1.1. To minimise WW asset and business risk;
1.2. To ensure that all of the WW computing facilities and services, programs and data are adequately protected against loss, misuse or abuse;
1.3. To create WW awareness that appropriate information and physical security measures are implemented as part of the effective operation and support of ICT facilities and services;
1.4. To ensure that all users fully comply with Information Security policy, standards, guidelines and procedures and the relevant legislation;
1.5. To ensure all users are aware of their responsibilities for the security and protection of facilities, services, programs and data over which they have control;
1.6. To ensure that the information security aspects of technology and business applications are consistent with the WW data protection policy and procedures

2. Responsibilities relating to the Policy

2.1. The WW committee/Board and Chair have the responsibility for the approval and review of all ICT-related policies, including this Information Security Policy;
2.2. The Chair oversees the overall strategic direction, management and operation of the WW's ICT operation and services, consistent with the operational objectives of the WW and has overall responsibility for information security and ensuring that users adhere to the agreed policy;
2.2.1. The Chair may delegate some aspects of this responsibility as agreed by the Board to a specialist IT Manager (employee or consultant) particularly relating to IT security;

2.3. The Chair must undertake regular risk reviews to ensure that all risks are identified and all reasonable measures are taken to prevent ICT security breaches;
2.4. All employees must assist in maintaining the security and integrity of the WW ICT infrastructure, facilities and services and have responsibility is to adhere to the WW related policies. (link to exact HR policy wording whenever possible)

3. Non-compliance or Breach of the Policy or any ICT related Procedure

Any breach of this policy will be managed in accordance with the ICT breach process detailed below. Disciplinary measures (as contained in relevant WW procedures and/or employee agreements) shall apply, for violations of this policy and any other policies or procedures associated with this policy.

4. General rules relating to Emails

Users shall apply the same personal and professional courtesies and considerations in electronic messages as they would in other forms of communication. Staff members are responsible for reading and complying with this procedure and any associated policies, procedures, guidelines or conditions of use. All email sent outside WW must have the following automatically attached insert relevant information e.g. Company Number, address etc.

In addition, Users:-

4.1. shall not transmit messages unnecessarily;
4.2. shall not transmit frivolous, abusive or defamatory messages;
4.3. shall not transmit electronic messages that are illegal or contravene other WW policies;
4.4. shall not make available to others or access themselves any content that they do not have rights to;
4.5. shall not cause interference with other users of email services; examples of interference include transmission of email chain letters, widespread distribution of unsolicited email, junk mail, pyramid mail and the repeated sending of the same message.

The WW email services may be used to send or receive incidental personal messages providing that such use will not:-

4.6. directly or indirectly interfere with WW business operations, or
4.7. interfere with the user's employment or other obligations to WW, or
4.8. cause or be likely to cause damage to WW's reputation, or
4.9. conflict with any WW policies, regulations or legislation

Commercial for profit activities or advertisements:-

4.10. WW's email services may not be used for commercial activities or personal gain, except as agreed by the Chair

4.11. Advertising or sponsorship is not permitted except where such advertising or sponsorship has been approved by WW Board

Email Property rights are reserved:-

4.12. all electronic messages stored on WW computers and networking facilities are deemed to be WW records and may be subject to disclosure if required by law;

4.13. all emails which are in support of WW business are considered to be a WW record, irrespective of the location or ownership of the facilities used to create or store the electronic record, Users of email services must be aware of their responsibilities in regard to the management, retention and disposal of WW records (refer to WW Data Management procedure)

Email Message Storage consent:-

4.14. by accessing the WW's email services, users consent to their electronic messages being stored both online and off-line as a part of routine WW system backup operations

4.15. under no circumstances is WW accountable for loss of personal electronic messages stored online or off-line

Email Privacy:-

Due to the nature of email systems, WW cannot guarantee the confidentiality of information contained in messages even though WW respects the privacy of Users:-

4.16. viewing of stored messages may be necessary from time to time, to help redirect messages that cannot be delivered, to examine contents for legal reasons, or for other operational purposes such as messages that cause failures in the system due to the presence of viruses, size, or message corruption;

4.17. WW permits the inspection, monitoring or disclosure of electronic messages without the owner's consent following Chair and Board authorisation only when-

4.17.1. consistent with and required by law;

4.17.2. there is substantiated reason to believe that violations of law or WW policy have taken place; or

4.17.3. in exceptional cases, to meet time-dependent, critical operational needs; or

4.17.4. it is necessary to protect the WW communication networks; or

4.17.5. emergency situations (e.g. when WW or its members are endangered or to maintain the integrity of information and services when access to email services must be secured to ensure the preservation of evidence) special dispensations apply

5. ICT Anti-Virus Software

5.1. WW will ensure that approved and maintained licensed anti-virus software from known and trusted sources is used on all computers owned or leased by WW;
5.2. anti-virus software must not be deactivated unless instructed to do so as part of a maintenance or similar procedure;
5.3. disciplinary actions may apply for violation of these procedures

6. ICT Breach Process

Any alleged breach of the ICT Policy must be reported to insert the chair who will record, investigate and act according to this process to ensure consistent and expedient investigation and management of alleged breaches.

Any incident that is considered to be an alleged breach of ICT policy or procedures will be categorised into:

6.1. Minor breach, or
6.2. Major breach

All breaches must be investigated to determine whether a breach was of an **accidental** or **deliberate** nature.

Consistent categorisation of breaches and recommended disciplinary actions across WW apply. Guides to the applicable response are described below:

Any information security incident where a legal infringement is suspected MUST be dealt with as a Major Breach.

Major Breach examples might include (but are not limited to):-

- Copying or sharing with others software, music or movies without the written permission of the copyright owner.
- Making a CD track or movie available via a file-sharing service or a web-site.
- Downloading a CD track or movie from a file-sharing service, a peer to-peer service, or a web-site.
- Storing a file on WW equipment that contains illegally copied software, music or video storing of files on a personal piece of equipment, copyrighted software or audio-visual material accessed using WW Internet service.

- Hacking into, meddling with, or damaging any other computer or service e.g. trying to “break into” or “crash” another computer on the Internet.
- Using another person's identity or authorisation codes. e.g., using someone else’s username or password.
- Possessing, accessing or using any unauthorised hacker tools, whether hardware or software based.
- Viewing, downloading, storing, sending, or giving access to material deemed as illegal.
- Harassing another person e.g. sending obscene messages, pictures or other materials; issuing threats of bodily harm; contacting a person repeatedly without legitimate reason; disrupting another person's lawful pursuits; and invading another person's privacy.

Minor Breach examples might include (but are not limited to):-

- Use of WW facilities and services for the playing of games

7. Standard for Password

WW has agreed a minimum standard for password setting and change is:

Amend based on the specifics of your system and/or supplier agreement

- Length of password (x) characters containing ….insert requirements e.g. letters, numbers, punctuation marks etc.
- Number of unsuccessful login attempts before the username is made inaccessible automatically (locked) x times
- Duration of lockout period xx minutes
- Period after which a password must be changed xx days/weeks/months

Users must not:

- Share their password with anyone
- Write their password down

A breach of these requirements may incur disciplinary action by WW.

8. Administrative Procedures on Ceasing Employment (or Key Volunteer Activity)

8.1. When a staff member’s employment with WW ceases for any reason, WW shall deny access by the former staff member to their electronic account(s).

8.2. When a key volunteer ceases to be involved, access to WW accounts and information shall cease. Any data held by the volunteer relating to their

volunteering must be returned to WW as soon as practicable or if returning of data is not required said data must be deleted from the key volunteer's equipment immediately, (particularly if the data relates to personal information of others e.g. a coach holding athlete personal information or a physio holding medical information).