



INTERNET ACCEPTABLE USE POLICY

- The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Ozarks Regional YMCA (ORYMCA) in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.
- Ozarks Regional YMCA provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

Definitions:

- “Users” are everyone who has access to any of ORYMCA’s IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.
- “Systems” means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

Scope:

- This is a universal policy that applies to all Users and all Systems. For some Users and/or some Systems a more specific policy exists: in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.
- This policy covers only internal use of ORYMCA’s systems, and does not cover use of our products or services by customers or other third parties.
- Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

- Staff members at ORYMCA who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

Use of IT Systems:

- All data stored on ORYMCA's systems is the property of ORYMCA. Users should be aware that the company cannot guarantee the confidentiality of information stored on any ORYMCA system except where required to do so by local laws.
- ORYMCA's systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However it must not be in any way detrimental to users own or their colleagues productivity and nor should it result in any direct costs being borne by ORYMCA other than for trivial amounts (e.g., an occasional short telephone call).
- ORYMCA trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain they should consult their manager.
- Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorized access is prevented (or at least made extremely difficult). However this must be done in a way that does not prevent—or risk preventing—legitimate access by all properly-authorized parties.
- ORYMCA can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.
- ORYMCA reserves the right to regularly audit networks and systems to ensure compliance with this policy.

Data Security:

- If data on ORYMCA's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information.
- Users are expected to exercise reasonable personal judgement when deciding which information is confidential.
- Users must not send, upload, remove on portable media or otherwise transfer to a non- ORYMCA system any information that is designated as confidential, or that they should reasonably regard as being confidential to ORYMCA, except where explicitly authorized to do so in the performance of their regular duties.
- Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with ORYMCA's safe password policy.

- Users who are supplied with computer equipment by ORYMCA are responsible for the safety and care of that equipment, and the security of software and data stored it and on other ORYMCA systems that they can access remotely using it.
- Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.
- All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.
- Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.
- Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, worms, backdoors) being imported into ORYMCA's systems by whatever means and must report any actual or suspected malware infection immediately.

Unacceptable Use:

- All employees should use their own judgment regarding what is unacceptable use of ORYMCA's systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.
- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities detrimental to the success of ORYMCA. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.
- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).



- All activities that are inappropriate for ORYMCA to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.
- Circumventing the IT security systems and protocols which ORYMCA has put in place.

Enforcement:

- ORYMCA will not tolerate any misuse of its systems and will discipline anyone found to have broken the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.
- Use of any of ORYMCA's resources for any illegal activity will usually be grounds for immediate dismissal, ORYMCA will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Policy Revision History			
Version:	Effective Date:	Authorized by:	Affected Provisions:
Version 0.1	06/12/2018	COO	--