October 2023

Technology and Computer Use Policy | Policy

POLICY OWNER:	Technology Department
POLICY APPROVED BY:	Chief Operating Officer & Director, Human Resources.
POLICY CONTACT:	Technology Department, help@water.org Director of Technology, kbridges@water.org

Policy Contents

I. Policy Overview

Policy Statement

This policy is intended to outline the rules and expectations related to the use of Water.org provided hardware and software.

Purpose

To enable employees to perform their jobs, Water.org ("the organization") provides employees with access to various electronic systems, software, and data. These electronic systems include voice mail, electronic mail (e-mail), facsimile (fax) transmissions, intranet, Internet, and computer networks. All communications and information transmitted by, received from, or stored on these systems are the property of Water.org, and as such are to be used for legitimate and authorized job-related purposes.

For this policy, a computer is defined as any system, server, workstation, or laptop computer, that runs an operating system including, but not limited to, Microsoft Windows. Devices included in this policy are Personal Information Devices (PDAs), Smart Phone devices, storage devices like USB drives and personal entertainment devices with the ability to store information in digital format. For this policy the term "computer" will refer to any of the above-mentioned devices.

Applicability

This policy applies to all Water.org personnel with organization provide assets and hardware or individuals with access to Water.org facilities.

Governance

The **Technology Department** is the owner of this policy and is responsible for administering, reviewing, and making recommendations for updates or changes to this policy in alignment with business needs.

Violations

It is the expectation of Water.org that direct supervisors proactively manage their direct reports' compliance with this Policy. Non-compliance, from an employee or a direct supervisor, may result in progressive disciplinary actions consistent with the organization's established HR procedures.

Every employee of Water.org is strictly accountable for the enforcement of this policy. Employees who violate this Policy are subject to disciplinary action up to and including immediate termination or any other remedy or remedies available under the law.

II. Policy

Information on computers should be protected from disclosure to, modification of or theft by unauthorized persons, and controls should be in place to minimize loss or damage. Users must take reasonable care in the use of the computer assigned to them by Water.org. Users assigned a laptop are responsible for its security, both physically and electronically (e.g., data residing on the hard drive). Water.org computers are to be used for the express purpose of conducting Water.org business. Any personal use of Water.org computers should be minimal and should not interfere with individual job responsibilities or with Water.org business operations. Management reserves the right to review all information stored and transactions occurring on Water.org infrastructure including servers, workstations, and laptops.

1. Requirements

1.1 Where appropriate, portable workstations and computer media should be stored in suitable locked cabinets or drawers when not in use, especially outside working hours.

1.2 Users should not store confidential information on the hard drive of the workstation computers or on other portable storage devices. Microsoft SharePoint Document Libraries and/or Microsoft Personal OneDrive should be used to store confidential information since appropriate access restrictions can be applied for such confidential data. Availability of information is also ensured by regular backup at the MS Cloud level.

1.3 Users should not download or install 3rd party or unapproved software on their computers without first checking with the technology department and gaining approval.

1.4 Computer games, dating and match making websites, pornographic websites and images/media, and chat rooms are strictly prohibited.

1.5 Sensitive or classified information, when printed, should be cleared from printers immediately.

1.6 The following control measures should be undertaken by the users to secure their personal computers from unauthorized access:

   a. Users should terminate or lock their logon session if they are leaving the computer system unattended.
   b. Hard disk(s) of the personal computer should not be shared.

1.7 Users may, with their manager's approval, use Water.org computers to access personal E-mail accounts and nonrestricted websites if said access does not impact the User's ability to adequately meet their job requirements.

1.8 Users are not permitted to make changes to Water.org's standard computer configuration unless approved by Technology.

1.9 Users should not store personal information on Water.org computers so that they would not be comfortable losing or having someone access.

1.10 The use of personal VPN software is not allowed unless approved by the technology team.

1.11 Users should keep food and drink away from workstations to avoid accidental spills.

1.12 If an employee plans on taking their work laptop with them to travel for personal reasons, they are required to inform the technology team (email help@water.org) as soon as they are aware of their dates and location.

1.13 User's onsite or working remotely must ensure that monitors are positioned away from public view when private, classified, or sensitive information is being viewed. If necessary, a privacy screen filter or other physical barrier to public viewing must be in place.

1.14 Users who are using personal equipment such as home laptops and personal smart phones which require connectivity to Water.org resources are expected to adhere to the same security standards and protocols as required on Water.org resources.

   a. Whenever possible, employees should use their assigned work laptop and/or smart devices when conducting business.
   b. If an employee must use a personal computer or smart device, access should be limited to the tools available in Microsoft 365 through an authenticated session.

1.15 For laptops, end users must employ a Water.org approved personal firewall or other compensating security measures deemed necessary by Technology.

1.16 Users must have an Water.org approved anti-virus and anti-malware software and the signature files / engines must be up to date (MS Defender for Windows/PCs and Malwarebytes for Apple/Mac).

1.17 Users must never disclose their passwords to anyone (other than the technology team) including family members if work is conducted from home.

1.18 Users are not to store Water.org confidential data on unencrypted workstations or mobile devices.

1.19 Users including employees and third parties will permanently erase Water.org specific data from workstations once their use is no longer required.

1.20 Users are required to immediately report to management, and the Technology and HR departments any incident or suspected incident of unauthorized access, data loss and/or disclosure, theft, or loss of Water.org information, resources, or devices. Users may be required to have follow-up actions, such as filing police reports, affidavit of loss, etc. Refer to the Security Incident Handling Policy and Procedure for ways to get in touch with the correct resource in an expedited manner.

1.21 Users are required to immediately report a lost or stolen workstation to management, and the Technology and HR departments. Refer to Security Incident Handling Policy and Procedure for ways to get in touch with the correct resource in the event of lost or stolen equipment.

2. Privacy and Water.org Information

2.1 Employees using these systems for personal purposes do so at their own risk. Although electronic messaging systems contain certain security features, Water.org does not offer, and employees should not expect privacy regarding any use of the electronic messaging systems. No encryption tool may be used, nor may any messages be encrypted internally or externally without the express prior written approval of Water.org's technology department.

3. Licensing and Software

3.1 Only licensed copies of software should be loaded to Water.org electronic systems by Water.org Technology Staff. A listing of all licensed software owned by Water.org is maintained by the Technology department. To ensure the use of these systems is consistent with Water.org's policies and legitimate business interests, authorized representatives of Water.org may monitor the use of such systems and the content of any data or software contained on such systems from time to time. Water.org data and information must be kept in Microsoft SharePoint Document Libraries and/or Microsoft Personal OneDrive. This information will be backed up daily. No data should be kept exclusively on individual computer hard disks i.e., "C" drives.

4. Password Confidentiality

4.1 Individual employees select passwords, including file passwords, but such passwords remain the property of Water.org. It is each employee's duty to protect the confidentiality of individual passwords which, if revealed inside or outside Water.org, could do great harm to Water.org's resources and investments. Please refer to the Identity Security Policy for more information.

5. Harrassment and Discrimination

5.1 Water.org's policies prohibiting all types of harassment and discrimination apply to the use of Water.org's electronic messaging systems. No one may use these electronic systems in a manner that may be construed by others as harassment based on race, national origin, sex, age, disability, religion, or any other characteristic protected by state or federal law. No jokes, oral or written statements, graphics or any other offensive, harassing, or discriminatory material may be transmitted over or stored on the electronic messaging systems. Please refer to for more information

6. Social Media

6.1 Water.org recognizes that social media and other online collaboration platforms are an effective way for individuals and organizations to communicate. This policy provides some practical guidance for responsible, constructive communications via social media channels for employees. Social media includes social networks, blogs, forums, wikis, and other websites where images, text and video are posted. Refer to the Standards of Business Conduct Policy for more details.

The guidelines are as follows:

1.0 Express only your personal opinions. Never represent yourself as a spokesperson for Water.org.
1.1 Do not use your personal account(s) to conduct official Water.org business.
1.2 Personal posts should not interfere with job responsibilities or be made using Water.org equipment.
1.3 If you are not an authorized spokesperson, you are not authorized to write on behalf of Water.org.
1.4 You are legally responsible for your internet postings, and you can be held legally liable if your comments violate applicable law.
1.5 You may also be personally liable if you make postings which include confidential or intellectual property protected information belonging to other parties.

4 Approval and Responsibility

Employee Responsibilities

The employee must follow the rules and expectations above to ensure a secure work setting.

Direct Supervisor Responsibilities

The direct supervisor must check that their direct report is using the company-provided technology safely. They must cooperate with Technology and HR Departments to fix or discipline any violation of the above rules or requirements.

5 Additional Resources

Contact for Support

You may ask questions to the Technology Department, help@water.org. For more personal or confidential questions or information please contact the Director of Technology, kbridges@water.org.

Related Policies

Identity Security Policy
Security Incident Handling Policy and Procedure