Staff Technology Acceptable Use Policy

	Last Review: 10/21/2021	**Next Review:** 10/2023
Approved by	Robert Willadsen , Brian Anders , Stephen Sweeney	
Created By	Kirk Bleavins, Director Technology & Business Solutions	

Reason for policy:

- ✓ **Security**
- ❑ **Compliance**
- ✓ **Knowledge management**
- ✓ **Stewardship**

Justification: JAARS uses electronic systems and devices to perform its mission, and JAARS staff rely upon these electronic systems and devices to perform their assignment. With ever-expanding technology capabilities, our use of technology will continue to grow and expand into all aspects of our assignments. All JAARS staff are expected to use electronic systems and devices responsibly and in appropriate ways that safeguard JAARS data, relationships, and reputation.

Policy

Electronic Systems and Devices

Ownership and Monitoring
JAARS provides electronic devices (e.g., computer, tablet, telephone handset), software, and access to electronic systems so staff may perform their assigned responsibilities. These systems, devices, and software are JAARS property. All data and communications sent from, received by, and stored on these systems and devices; passwords; and encryption keys are JAARS property. Staff must return system access, devices, and software to JAARS upon request or termination of your employment or assignment.

JAARS monitors its electronic systems and devices. Staff do not have personal privacy rights on JAARS systems or devices, nor are privacy rights granted to staff's personal devices that attach to JAARS networks or systems.

Inappropriate Use
Inappropriate use of JAARS systems and devices may result in loss of access privileges, loss of devices, and corrective actions (section 325), as well as, possible legal action. Examples of inappropriate use include:

- Using JAARS systems or devices for commercial activity for personal gain.
- JAARS systems, including email, are not for personal use. It is expected people have personal accounts for personal communications and systems.
- Unauthorized access to others' accounts and data. Attempts to gain unauthorized access to others' accounts or data (e.g., hacking).
- Misrepresenting yourself by sending information from someone else's account.
- Abusing JAARS systems and devices by causing excessive strain (e.g., large file downloads); misusing or destroying information contained on JAARS systems and devices.
- Unauthorized sharing of JAARS, its partners', or its constituents' confidential information

(e.g., email addresses, contact information, mailing lists, financial data).
- Sharing your credentials (username and/or password) with others.
- Efforts to inhibit JAARS authorized monitoring of or access to JAARS systems and devices.
- Use that violates JAARS policy or North Carolina, United States, or international law.
- Use that creates or disseminates information that detracts from the reputation of JAARS or its partners.
- Creating, distributing, or using unauthorized copies of copyrighted materials.
- Sending or forwarding obscene or harassing messages (e.g., hate mail, obscenity, ethnic or racial slurs, inappropriate jokes).
- Accessing sexually oriented websites; the receiving, storing, or sending of sexually oriented material.
- Sending, forwarding, or receiving communications of political nature using JAARS systems, devices, or accounts (e.g., your jaars.org email account). Examples of political communications are petitions, political campaign material, information that endorses candidates and links to political websites.

Internet Monitoring and Content Filtering
JAARS monitors Internet usage and uses content filtering to block objectionable Internet sites to maintain a spiritually healthy work environment. Attempts to access a blocked site are recorded and periodically reviewed. Intentional attempts to access filtered sites may lead to corrective action.

Support for Personal Devices
JAARS staff may use personal devices (e.g., personal mobile devices or home computers/laptops) to access JAARS data but staff is personally responsible to setup and configure the devices. JAARS technical support and configuration is limited to JAARS issued electronic devices.

RACI Chart (Roles and Responsibilities Matrix)

	General Staff	Dept. Directors	TBS Infra. Manager	Tech Director	People VP	TBS VP
Creation	NA	NA	R	A	C	C
Approval	I	I	C	C	C	AR
Enforcement	I	I	R	A	C	C

R = Responsible, A = Accountable, C = Consulted, I = Informed; see RACI Ref Doc for details

Related Policies and Procedures

JAARS HR Handbook
Tenant Acceptable Use - Policy

Research/References