100 Acceptable Use Policy v2

100 ACCEPTABLE USE POLICY

100.1 Introduction:

This Acceptable Use Policy (AUP) outlines the guidelines and expectations for the use of technology resources provided by the Archdiocese of Baltimore. All users, including employees, volunteers, contractors, and any individuals granted access to the organization's technology resources, are required to adhere to this policy.

100.2 Purpose:

The purpose of this policy is to ensure the appropriate and responsible use of technological resources, including computers, networks. internet access. email, and other electronic communications systems. By following this policy, we aim to protect the organization's information assets, maintain the integrity of our systems, and promote a respectful and productive technology environment.

100.3 General Guidelines:

3.1. Compliance: Users must comply with all applicable laws, regulations, and policies governing the use of technology resources.

3.2. Authorized Use: Technology resources provided by the organization are to be used for official purposes and activities related to the organization's mission. Personal use should be limited and should not interfere with work responsibilities.

3.3. Access Control: Users are responsible for safeguarding their login credentials and preventing unauthorized access to their accounts or any confidential information.

3.4. Security: Users must not attempt to bypass security measures, install

unauthorized software, or engage in any activity that may compromise the security or integrity of the organization's systems.

3.5. Privacy: Users should respect the privacy of others and refrain from accessing, using, or disclosing any confidential or personal information without proper authorization.

3.6. Intellectual Property: Users must respect intellectual property rights and should not copy, distribute, or use copyrighted material without proper authorization.

100.4 Internet and Email Use:

4.1. Internet Use: Internet access should be used for work-related purposes. Inappropriate websites, including those containing explicit, offensive, or illegal content, should not be accessed.

4.2. Email Use: Email should be used for official communications and should adhere to the organization's Email Policy. Users should exercise caution when opening email attachments or clicking on links from unknown or suspicious sources.

100.5 Social Media and Online Activities:

5.1. Social Media Use: Users should represent the organization professionally and responsibly on social media platforms. Confidential information or sensitive organization matters should not be shared without proper authorization.

5.2. Online Behavior: Users should engage in respectful and ethical online behavior, refraining from engaging in cyberbullying, harassment, or any other form of harmful or malicious activities.

100.6 Consequences of Violations:

Violations of this policy may result in disciplinary action. including but not limited to verbal or written warnings, temporary or permanent loss of technology privileges, and termination of employment or volunteer status. Legal actions may also be pursued if violations involve illegal activities.

100.7 Policy Review and Updates:

This policy will be reviewed periodically and updated as necessary to address emerging technology trends, legal requirements, and organizational needs. Users will be notified of any policy changes, and they are responsible for familiarizing themselves with the current version of the policy.

By using the organization’s technology resources, users acknowledge that they have read, understood, and agree to abide by the terms and conditions outlined in this Acceptable Use Policy.