Archdiocese of Seattle (CCAS)

Technology Acceptable Use Policy

Final

January 2024

Table of Contents

Technology Acceptable Use Policy

Summary

This policy describes the principles of acceptable and unacceptable use of internet, hardware, software (including software as a service) and other technology ("resources") provided or licensed by The Archdiocese of Seattle, including the Chancery, parishes, Cemeteries and schools or the Corporation of the Catholic Archbishop of Seattle ("CCAS").

These resources are provided to employees and authorized persons affiliated with CCAS ("users") for the efficient use of applications and the exchange of information as they carry-out their assigned responsibilities and for the benefit of the Archdiocese of Seattle. Use of these resources is expected to be consistent with the mission and official work of CCAS and its security and confidentiality policies.

The policy defines CCAS' rights and establishes enforcement and violation provisions. Employees and users granted access to these resources are required to attest in writing they have read and agree to abide by this policy.

Resources include but are not limited to the following types of devices and services:

- any endpoint such as a desktop and portable computer/laptop, virtual machines, tablets or mobile devices
- network services such as the internet and intranet,
- electronic data such as email, messaging and file sharing,
- business applications (including those hosted by a third-party) and
- printers, copiers and faxes
- any computing peripherals such as cameras and conference room AV equipment.

Users accept use of these resources creates certain exposures and security risks, legal liability, and operational and reputational risks. Users agree to conduct themselves on the internet and while using CCAS provided resources in a manner that does not introduce or elevate CCAS' security risk, legal liability or expose CCAS to operational or reputational risks.

Acceptable Use

The use of the CCAS resources is for the benefit of the Archdiocese of Seattle and for authorized purposes only. Users agree to act responsibly and abide by the following principles:

1. Respect and be considerate of others. Users shall not intentionally interfere with or seek information on, obtain copies of, or modify files or data maintained by other users, unless explicit permission to do so for official reasons has been obtained.
2. Adhere to state and federal laws, Archdiocesan policies and regulations and the teachings and mission of the Catholic Church.
3. Adheres to any other applicable or related policy for which the user is subject to including (but not limited to) records retention schedules and Archives & Records Management policies and system authorization and access policies.

4. Abide by copyright, patent, and trademark laws and license agreements for software, digital artwork, fonts, or other forms of electronic information and asset protection.
5. Protect the integrity of the CCAS resources and safeguard data from unauthorized use or disclosure.

Unacceptable Use

Users may not use CCAS resources to conduct or engage in illegal or harmful activities or any other behavior that is in contradiction or unrelated to the mission of the CCAS. Types of unacceptable use include (but are not limited to) the following:

- Activities unrelated to official assignments and/or job responsibilities, except incidental personal use (see below) in compliance with this policy, including but not limited to storage of files or media or use of CCAS computing resources.
- Activities related to private purposes, whether political, personal gain, for-profit or non-profit, such as marketing or business transactions unrelated to Archdiocesan duties.
- Transmitting profane, pornographic, obscene, threatening, or harassing materials or correspondence.
- The exercise of a users' right to free speech. Resources are not to be used as an open forum to discuss policy, organizational or business matters.
- Creating hostility. Any sexual, ethnic, or racial harassment, including unwanted telephone calls, electronic mail or messaging, is strictly prohibited.
- Unauthorized or unsecure distribution of CCAS data and information (e.g., emailing sensitive, confidential or personally identifiable information to recipients not authorized to receive such information or to authorized recipients in an unencrypted form).
- Interfering with or disrupting users, services or equipment, including cybersecurity devices, software and services.
- Advocating religious beliefs or practices contrary to the mission and teachings of the Catholic Church.
- Licensing, uploading or downloading commercial software without prior authorization of the Archdiocese and/or in violation of its copyright.
- Intentionally violating security policies or putting the Archdiocese at risk for cybersecurity threat or that would subject CCAS to loss or liability.
- Misrepresenting, obscuring, suppressing, or replacing their own or another user's identity on an electronic system.
- Release of any media announcement, advertisement, internet page, social media post, electronic message, voice mail message, or any other public representation about the CCAS unless it has been approved by the Office of Communications.
- Other department, site or work unit specific guidelines in addition to the above.

Personal Use

Users agree CCAS resources are to be used primarily for the benefit of the Archdiocese of Seattle. However, CCAS does understand and acknowledge that its employees may make reasonable incidental use of CCAS resources for appropriate personal use. Appropriate personal use includes activities that do not impact overall work performance but need to take place during normal work hours.

Excessive personal use of CCAS resources is the judgment of the supervisor or human resources. CCAS Information Technology Services can monitor for inappropriate or excessive use such as that which

results in expense, service degradation, security exposure or breach and data or other loss to CCAS. Violations of excessive personal use are subject to the enforcement provisions of this policy.

Use of Electronic Mail, Messaging, File Sharing Systems and Cloud Services

Users agree to only use CCAS authorized and provided electronic email, messaging, file sharing software and Cloud Services for CCAS work. Unless permission from the Chief Information Security Officer has been obtained, users may not use external personal email accounts or unauthorized file sharing for the exchange of information, files or data for any CCAS work.

Intellectual Property Rights

Use of CCAS resources to repost or reproduce protected materials may only be done so after obtaining permission from the authorized source and only if the source is properly represented and identified.

Unless third parties have clearly noted copyrights or some other rights, data or programming products handled by or developed by CCAS staff through these resources, are the property of CCAS. No user may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software and without express authorization from CCAS.

Limitation of Liability

CCAS makes no warranties, either express or implied, regarding protections, software or information obtained from the internet. CCAS resources, including internet access, are provided on an as is, as available basis.

CCAS is not responsible for any exposure or damage resulting from the use of its computers, network or information systems resources. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of the internet and of any information obtained from the internet is at the user's risk. Users are responsible for protecting their own privacy.

CCAS reserves the right to remove from its information systems resources any material it views as offensive or potentially illegal at any time.

CCAS reserves the right to inspect any data and files stored anywhere on the network or on individual endpoints such as personal computers or storage media for any necessary deemed purpose or to ensure compliance with policy and state and federal laws. Users are aware all information stored on, entered, or transmitted in any way through the CCAS resources including the network and owned and managed devices, including but not limited to electronic mail messages sent and received using CCAS resources, are not private and are subject to monitoring, logging, viewing, downloading, inspection, release, and archiving by CCAS officials at all times.

With the exception of authorized Information Technology Services and Records Office personnel, no employee may access another employee's device, computer files, or electronic mail messages without prior authorization from an appropriate CCAS official.

CCAS reserves the right to log network use and monitor storage space utilization and assumes no responsibility or liability for files deleted due to violation of storage space allotments.

CCAS reserves the right to revoke user access from the resources without notice.

CCAS reserves the right to change its policies and rules at any time.

Use of Personal Devices (BYOD)

Users who access CCAS resources from a personal computing device (computer, tablet, phone, etc.) for work- or business-related activities must do so in accordance with this policy and all other related CCAS policies, laws and regulations. This access and its proper use are obligations of employment when they are granted in order to fulfill the responsibilities of the position. CCAS does require some employees to use personal equipment for business reasons but is not responsible for the purchase or costs associated of this use.

Users must:

- Register the personally owned device under the users own account(s)
- Abide by CCAS passphrase protections such as strong passphrase, multi-factor authentication (MFA)
- Not store CCAS confidential, Personally Identifiable Information or Sensitive Information on personally owned devices.
- Not access Personally Identifiable Information or Sensitive Information from personally owned devices except through applications designed to do so in accordance to these policies.
- Destroy, remove, or return all data, electronic or otherwise belonging to CCAS once their relationship with CCAS ends or once they are no longer the owner or primary user of the device. (e.g., the sale or transfer of the device to another person).
- Remove or return all software application licenses belonging to CCAS once the application is no longer being used, the users' relationship with CCAS ends or once they are no longer the owner or primary user of the device. (e.g., the sale or transfer of the device to another person).
- Notify the CCAS Information Technology Services of any theft or loss of the personal device containing data or software application licenses belonging to CCAS.
- Not connect any personally owned device to secure CCAS networks without prior authorization.
- Not compromise the device operating system or components (i.e., jailbreak)
- Be current on all software updates and anti-virus solutions.
- Not synchronize CCAS information on the personally owned device with other personal devices or other personal cloud-based storage or access unsecure internet sites.
- Refrain from using their personal computing devices while operating a vehicle. Employees who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

CCAS may employ the use of Mobile Device Management (MDM) software to be installed on personal devices to keep company-related information all in one secure space on the device, which is then passphrase-protected. MDM may also be used to enforce certain security parameters of the personally owned device such as minimum passphrases, inactivity lock, etc.

CCAS reserves the right to, without notification, revoke access, prevent or ban any access from personally owned devices at any time for any reason. This can include remotely wiping a personally owned device if it is lost or stolen.

Grave care must be exercised in using IT systems in the course of your work when you are entrusted with peoples' personal, private information as a mistake can be broad and wide in scope and may expose you to personal liability whether the release of information was intentional or by accident. Employees may be individually liable for any and all damages incurred as a result of violating the Archdiocese of Seattle security policy, copyright, and licensing agreements.

Exempt employees are expected to be able to be accessed by phone as required by their job responsibilities. This may require publishing their personal phone number in appropriate directories as designated by the employer. Work phone access may be extended to the personal phone via Voice over IP applications as needed to ensure the employee meets job responsibilities.

Reporting Requirements

Users must promptly report any known loss of CCAS resources and data, information security alerts, security vulnerabilities, warnings, or problems. School and parish users should report such issues to their location IT Support team and the location administrative leader (PAA, principal, or school leader). Chancery staff should report to the Help Desk, x4351 (206-382-4351 or helpdesk@seattlearch.org).

Users who receive offensive electronic mail messages, telephone calls, or other electronic communications, must report the activity to their location IT support and as necessary to their supervisor or Human Resources department immediately.

Users who receive offensive unsolicited material from outside sources must not forward or redistribute it to either internal or external parties unless this forwarding or redistribution is to the Human Resources department or to the location IT Support to assist with the investigation of a complaint.

Enforcement and Violations

This policy is intended to be illustrative of the range of acceptable and unacceptable uses of Internet facilities and is not intended to be exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of specific unacceptable uses should be directed to the user's supervisor or human resources. CCAS will review alleged violations of this policy on a case-by-case basis. When a supervisor becomes aware that an employee may have violated this policy, the following may occur:

1. CCAS may immediately place the employee on administrative leave pending the outcome of an investigation.
2. The Human Resources department may notify location IT Supports to immediately block access system-wide to any website or database found to contain material that violates this policy; they may also determine whether a report to law enforcement is required and/or a forensic investigation of all CCAS resources used by the employee is warranted.

Violations of the policy may result in disciplinary actions as appropriate, up to and including dismissal. CCAS will cooperate with requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual internet activities, e-mail use, and/or computer use.