

01.00.00: KofC Council 12480 Acceptable Use Policy

This document describes what is and is not acceptable use of KofC Council #12480's Information Technology Environment. This includes computers, email, networks, phones, and other electronic means.

Procedures supporting this policy:

- [Mass Email Procedure](#)
- [Instant Messaging Security Procedure](#)
- [Email Security Procedure](#)
- [Encryption Process Procedure](#)
- [Software Licensing Compliance Procedure](#)

Purpose

Effective 07/01/2005, supercedes any previous versions of Internet Acceptable Use Statement.

Council business information is an essential asset of KofC Council #12480. This document:

- States what is and is not acceptable use of these resources
- Defines the responsibilities of those who handle these resources
- Defines the penalty for misuse of these resources

Scope

This policy covers all persons or organizations that come into contact with council information assets by means of responsibility, business contact, or coincidence. For purposes of this policy, information assets used or produced by council members are to be treated like they are owned by council members.

Who is Affected

Each Brother Knight or other party that comes into contact with council Information Assets, whether on Church premises or not, is affected by this policy.

Requirements

1. Authorized Usage

Defines what acceptable use of KofC Council 12480's resources is.

Council information assets must be used primarily for council business activities.

Incidental personal use is allowed so long as:

- it doesn't consume more than a trivial amount of resources
- it doesn't interfere with staff productivity
- it doesn't pre-empt any council business activity

2. Unacceptable Use

Don't use council resources in any way that would create the appearance or reality of inappropriate use.

It is unacceptable to use council information assets to actively engage in creating, procuring, or transmitting any materials that are in violation of KofC Values, Policies, or local laws. The KofC's Values are located at <http://www.kofc.com>. Examples of items that are not acceptable based on those policies are (but are not limited to):

- Derogatory racial comments
- Sexual content (pornography)

- Derogatory religious comments
- Offensive language
- Any material which would negatively reflect upon the KofC
- Defamation or derogatory/abusive attacks on any individual/group

You should not use information resources for private business activities unless expressly approved by council officers. You should not create either the appearance or the reality of inappropriate use of council resources.

You should not attempt to:

1. Access resources that you don't have valid access to.
2. Circumvent security measures with other technology.
3. Utilize "hacking tools" to probe or attack system vulnerabilities.
4. Violate rights protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
5. Make unauthorized copies of copyrighted material including the installation of any copyrighted software for which you or the council doesn't have an active license.
6. Export software, technical information, encryption software or technology, in violation of international or regional export control laws. Check with council officers for further clarification of the legal issues.
7. Introduce malicious programs into the environment (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
8. Make fraudulent offers of products, items, or services from a council account.
9. Make statements about warranty, expressly or implied, unless it is a part of normal job duties from a council account.
10. Provide information about, or lists of, council members to 3rd parties.

If you are using a council computer or communications system (e-mail, ftp, instant messaging, online chat, or other Internet Services), you should **not**:

- Use e-mail for spamming (unsolicited, indiscriminate mass mailings)
- Use Internet streaming technologies (audio or video) except for specific council business purposes
- Use multi-player gaming technologies except for specific council business purposes
- Upload or post any political statements not sanctioned by the council officers
- Download or use any hacking, sniffing, or probing devices/software unless approved by council officers

5. User Responsibilities

If you get a file from the Internet, check it for viruses and Trojan horses.

All software downloaded from the internet, including Microsoft Update, must be screened with council approved virus detection software prior to being opened or run on a council system. If there is not a virus detection tool available for your platform, then the software should be run and tested on a stand-alone system before being loaded to a council system. You should look for expected behavior and verify no other activities happen when you are testing the software from a non-council source.

6. Encryption

You are responsible for securing council sensitive data.

Information assets are not encrypted by default. We require that any information that is classified as private or information that you consider sensitive or vulnerable must be encrypted before being transmitted. This includes transmission of data over the internet.

7. Proprietary Information

Don't share information without proper approvals.

You bear the responsibility for taking the necessary precautions to ensure the privacy and integrity of council business information. You should not post council sensitive data on any public forum without specific approval from the council officers. If you have questions about how to handle or share any type of council business information or what the local laws require, contact the council officers.

8. Respecting Privacy Rights

Information on council information assets may be read in the process of maintaining the servers and infrastructure.

Users may not intercept or disclose, or assist in intercepting or disclosing, information assets, unless specifically approved by council officers. Our council is committed to respecting the rights of its members, contractors, and business partners.

The council is responsible for maintaining and protecting its information assets. To do this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, business information.

9. No Guaranteed Privacy

Don't assume privacy in the Internet world.

The council cannot guarantee that storage or transmission of information assets will be private. You should be aware that, depending on technology, information can be forwarded, intercepted, printed, and stored by others. Others can access information assets in accordance with this policy.

10. Monitoring

Information assets are monitored to meet operational and legal requirements.

The council routinely monitors council information assets. The council does not regularly peruse individual files or packets on its information assets. The content may be monitored and the usage of the systems will be monitored to support operations, maintenance, audits, security, and investigations. If during the course of system work, evidence of abuse is uncovered, it will be investigated. You should structure your use of information assets in recognition of the fact that they might be examined. Monitoring will meet local law requirements/restrictions.

11. Incidental Disclosure

Your document may be read during normal infrastructure work activities.

It may be necessary for council officers to review the content of an individual's communications or other information assets during their normal work activities. This information should not be disclosed to anyone. Council officers may not review the content out of personal curiosity or at the behest of others who have not received proper approval from the council officers.

Responsibilities

- You are responsible for the maintenance of the assets in compliance with this policy, the standards and procedures, and other processes the council officers might see fit to implement. You are responsible for protecting council information from accidental or intentional unauthorized:
 - access
 - modification
 - duplication
 - destruction
 - disclosure
- Chairmen must support this policy and ensure that their team members comply with this policy and its support documents.
- The Webmaster must prepare and maintain this document. Additionally they must implement the measuring and monitoring of information assets to ensure compliance with policies, standards, and procedures.
- The council officers must implement and support this policy.

Enforcement & Exception Handling

Unauthorized acts against the council, its business partners, or the Church will result in disciplinary action, including suspension, as deemed appropriate by the council officers. These actions include, but aren't limited to:

- misuse
- misappropriation
- misrepresentation
- destruction of information or system resources
- deliberate or unauthorized disclosure of information

The Deputy Grand Knight (or a delegate) will evaluate exceptions and approve as appropriate.

Approval

Council Officers

Change Management Record

Date	Who	What	Where

Web Resources:

<http://www.kofc.org/agreement.cfm>

<http://www.kofc.org/publications/columbia/detail.cfm?id=4366>