

Safeguarding

Ukrainian Catholic Eparchy of Saskatoon 214 Ave. M South, Saskatoon, SK, S7M 2K4 CANADA

Tel: 306-653-0138 x. 228 Cell: 306-222-1475

E-mail: safeguarding@skeparchy.org

Web: https://www.skeparchy.org/wordpress/about-us/policies-andprocedures/eparchial-covenant-of-care-abuse-and-misconduct-policy/ APPENDIX G: Electronic Communication and Technology Code of Conduct Reference Sheet (Page 1 of 4)

ELECTRONIC COMMUNICATION AND TECHNOLOGY CODE OF CONDUCT

Employees and volunteers must abide by the following rules and procedures in all electronic communication within their roles serving the Eparchy.

- 1. All parish and ministry websites, blogs, and social networking accounts are to be protected by a password, known by at least two adults and held in confidence. The webmasters/administrators must be adults (i.e. at least 18 years of age). Passwords for all parish websites, blogs, or social networking accounts must be known to the Pastor/Administrator and the person(s) appointed to be the webmaster/administrator.
- 2. All material placed on parish websites, blogs, and social networking accounts shall be supervised by the Pastor/Administrator, who is responsible for monitoring, accessing, updating, and editing that specific account's activity and content when necessary. For websites, blogs, and social networking accounts for other ministries, an Eparchial employee or member of the clergy must be one of the administrators on the account to carry out the aforementioned responsibilities. Initiation of such sites, pages, and accounts must have the prior approval of the proper supervisor and be registered with the Eparchy or parish.
- 3. Lists of parishioners and their donations is not to be posted online. If the parish bulletin contains such information, the information is to be deleted or blacked out before the bulletin is uploaded.
- 4. Material of a political nature such as supporting or opposing a candidate or political party in Canada or abroad is not to be found on a website, blog, or social media account of the Eparchy, a parish, or any ministry.
- 5. Where comments are enabled, the following must be included in an immediately visible place:
 - "All posts and comments should be marked by Christian charity and respect for the truth. They should be on topic and presume the good will of other posters. Discussion should take place primarily from a faith perspective. No ads please.
 - Persons who do not abide by this code of conduct will be blocked." Trust your instincts in blocking anyone who does not abide by this code of conduct, particularly repeat offenders.
 - In particular situations, it might be best to ask a member to take a conversation "offline." These offline conversations can be conducted in person, over the telephone, or through private email. The poster can be referred to appropriate resources, such as the Pastor/Administrator, a program director, the Eparchial Communication Office, etc.
- 6. When commenting, write in first person. Do not claim to represent the official position of the organization or the teachings of the Church, unless authorized to do so.
- 7. When commenting, identify yourself. Do not use pseudonyms or the name of the parish, ministry, etc., as your identity, unless authorized to do so.
- 8. Webmasters/administrators are not expected to respond to defamatory, libelous, or slanderous comments. The Eparchial Communications Office will provide a response to major news breaks when events require.
- 9. Electronic communication shall not contain obscene, harassing, threatening, abusive, crude, sexually suggestive, derogatory, defamatory, illegal, or otherwise potentially scandalous comments, links, and/or images which reflect negatively on, discredit, or cause embarrassment to the Eparchy and/or the faithful.
- 10. Maintain appropriate relational and ministerial boundaries in all forms of interaction and communication, especially with minors and vulnerable adults. See: *Eparchial Covenant of Care*.
- 11. Never access, post, or send pornography (adult or minor) of any kind to any person. (The definition of pornography as per the *Abuse and Misconduct Policy* is applicable.)
- 12. Accounts, groups, and/or pages for a parish, office, or ministry should clearly be named and operated as such; they should be separate from personal accounts. This includes social media accounts, groups, and pages.

Safeguarding



Ukrainian Catholic Eparchy of Saskatoon 214 Ave. M South, Saskatoon, SK, S7M 2K4 CANADA

Tel: 306-653-0138 x. 228 Cell: 306-222-1475 E-mail: safeguarding@skeparchy.org

Web: https://www.skeparchy.org/wordpress/about-us/policies-andprocedures/eparchial-covenant-of-care-abuse-and-misconduct-policy/

APPENDIX G: Electronic Communication and Technology Code of Conduct Reference Sheet

(Page 2 of 4)

- 13. Treat all communication as if it were public. Communication through these forms of technology does not always remain private.
- 14. Set and maintain privacy settings in every social media platform. As these may change as the platform evolves; recheck them occasionally.
- 15. Eparchial, parish, or ministry web pages, blogs, or social networking accounts shall not be used for conducting outside/personal business.
- 16. Employees and volunteers are prohibited from disclosing information that is proprietary to the Eparchy or understood to be held in confidence by the Eparchy and all relevant provincial and federal laws through any means of electronic communication, except by explicit permission of the appropriate authority.
- 17. All electronic communication must comply with Canada's anti-spam legislation and all other applicable federal and provincial laws.
- 18. Email addresses should not be released without permission, and thus the bcc (Blind Carbon Copy) function should be utilized when possible. This means that senders' email to their own address with other emails sent in the *bcc* box provided in all email software.
- 19. Common courtesy demands that one does not forward emails without permission of the sender and when forwarding emails, persons so doing must delete the address of the sender before forwarding, unless specific permission to share address information has also been granted by the sender.
- 20. If, at any time, an employee or volunteer receives an inappropriate personal communication from anyone participating in or affiliated with the Eparchy, parish, or ministry, the individual should maintain an electronic copy, print a hard copy, and notify a supervisor immediately.

Communication with minors and vulnerable adults:

- 1. Parents/legal guardians must designate, in writing, which form(s) of communication with minors may be used and must provide the contact information as well as contact information for parents/legal guardians. (All subsequent references to parents apply equally to legal guardians.) Parental permission must identify the type of communication (e.g. email), the minor's contact information (e.g. email address), and contact information for parents/guardians. Parents should also be made aware that they can opt out of allowing their children to be contacted through these means. Parents must have access to all communication provided to minors. All communication and information provided to minors through any electronic means is to be made available to parents through some means of communication, electronic or otherwise. **Social Networking Consent Form** (Appendix L).
- 2. For official ministry communication, there must be at least two adults with administrative rights for each social media account, page, or group. Only designated social media accounts, groups, or pages are to be used for ministry communication with minors.
- 3. To protect minors, at least two adults with appropriate authority are to be present for any interaction with a minor. Appropriate authority means approved by the Eparchy for ministry with minors or the minor's parent/guardian. That is, every correspondence between an adult and a minor will have a second adult present and/or electronically copied. If a minor individually contacts a particular adult engaged in ministry (other than a "friend" request), the ministry account should be used to reply by sending a group message (e.g. when the reply is relevant to all in the group). When a group response is not appropriate, the adult is to avoid using a social media account to respond. In exceptional cases when social media is used to respond, adults should maintain copies of all such messages.
- 4. The purpose of this electronic communication is to provide information related to ministry, an educational activity, or an event, not for socialization or other personal interaction. Counseling minors or vulnerable persons through electronic communication is not permitted. Prolonged conversations or interactions of a personal nature with minors through such communication methods are prohibited. Family members and godchildren are exempt.
- 5. Employees and volunteers will not share personal cell phone numbers with minors unless approved by parents and supervisors.

Safeguarding



Ukrainian Catholic Eparchy of Saskatoon 214 Ave. M South, Saskatoon, SK, S7M 2K4 CANADA

Tel: 306-653-0138 x. 228 Cell: 306-222-1475

E-mail: safeguarding@skeparchy.org

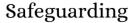
Web: https://www.skeparchy.org/wordpress/about-us/policies-andprocedures/eparchial-covenant-of-care-abuse-and-misconduct-policy/ APPENDIX G: Electronic Communication and Technology Code of Conduct Reference Sheet

(Page 3 of 4)

- 6. Communication with minors must utilize the *bcc* function (see number 18 above).
- 7. Except in an emergency, electronic communication between employees and volunteers and any minor participant(s) should take place between the hours of 6:00 a.m. and 10:00 p.m. including posting to websites and social networking sites. Employees and volunteers are reminded that many applications have ways to delay communication being sent.
- 8. On public ministry accounts or pages that include minors, the "no tagging" (or similar feature that avoids a direct link with a minor's personal social networking profile) should be set wherever possible.
- 9. Live chat or video conferencing without a second adult present is prohibited, as there will be no permanent record of what was transmitted unless it was recorded in real time. Family members and godchildren are exempt.
- 10. When using a ministry social media account, adults must not initiate "friend" requests with minors as they may feel unable to decline this request given the adult's position of authority.
 For this reason, clergy should likewise not initiate "friend" requests with minors, even on their personal accounts. Adults may accept "friend" requests from children who are involved in the particular ministry.
- 11. When minors form their own social media groups, adults are not to join.
- 12. When minors serve in a position of trust, for the duration of their employment or volunteering, they are not to engage in electronic communication with those with whom they have a ministerial relationship unless that electronic communication is copied with two adults with appropriate authority as specified in page 19, number 3. Additionally, these minors in a position of trust are not to post still or video images of other minors with whom they have a ministerial relationship on personal websites, blogs, social media accounts, or in other forms of personal electronic communication.
- 13. The above provisions apply to the use of social media and electronic communication with vulnerable adults when those persons have a legal guardian. If there is no form of legal guardianship but there are still indications of vulnerability (as per the definition of "vulnerable adult" in the *Abuse and Misconduct Policy*) those in ministry must either have another adult be party to all communications and/or maintain copies of these communications (electronically or otherwise).

Photography and videos:

- 1. It is commonly accepted that attendance at a public event such as a Divine Liturgy or a parish celebration may result in still or video images that may be used in social media, websites, or other public communication. Wherever possible, employees and volunteers should make every attempt to obtain consent from participants. In the case of an individual or small group (e.g. a family) during a sacrament (e.g. baptism), still or video images should only be for a specific purpose and with advance permission.
- 2. The posting or utilization of any personal information, including still or video images of minors, without obtaining the consent of a parent/guardian is prohibited. Personal information includes full name, home address, telephone number, email address, images, recordings and/or any detail that would allow someone to identify or contact a minor. Consent can be obtained through a release/waiver form, an email from a parent or guardian, or by spoken permission with another adult present. For our purposes, the following individuals should provide consent: parents or guardians are to consent for minors, and adults should consent for themselves.
- 3. It is recommended that for any ministry or event requiring a registration or permission form, a clause seeking permission to post still or video images from such activities on an Eparchial, parish, or ministry website or social media channels be included. A statement with a simple check box should suffice.





Ukrainian Catholic Eparchy of Saskatoon 214 Ave. M South, Saskatoon, SK, S7M 2K4 CANADA

Tel: 306-653-0138 x. 228 Cell: 306-222-1475

E-mail: safeguarding@skeparchy.org

Web: https://www.skeparchy.org/wordpress/about-us/policies-andprocedures/eparchial-covenant-of-care-abuse-and-misconduct-policy/ APPENDIX G: Electronic Communication and Technology Code of Conduct Reference Sheet (Page 4 of 4)

4. If Church services are to be recorded by any means, and/or if there is to be any public access, either online or by other means to these recordings, there must be signs clearly posting this fact at each public entryway in a manner that the ordinary person would not miss. It must be on a sign that is easy to read, placed in the middle of each entry aisle. Signs above or on doors or on a bulletin board off to the side will not be considered adequate notice. Church spaces that livestream either events or continuous feed to any public internet platform must likewise maintain adequate signage, as per the above requirements, at all times the feed is live. Those who opt for continuous feed or recordings must also be sensitive to the desires of parishioners and clergy who may not wish to have particular events streamed or recorded. While our Churches are public spaces there may be times when this sort of sharing is inappropriate, especially if it involves safety concerns.

Movies/Films:

- 1. Provincial ratings are to be adhered to as part of any catechetical program for children and youth as well as, if applicable, camp policy. All viewers must be older than the group for which the film is classified.
- 2. The persons selecting the films will also avoid movies with content advisories of severe violence, nudity, and a great deal of crude language or behaviour that is in any way demeaning to human dignity, especially when being shown to minors.
- 3. If the supervisors/catechists decide to show clips as part of a lesson or catechetical teaching from movies that are above the designated rating or with objectionable content, they may, if the objectionable parts are removed.
- 4. All movies must be "pre-screened" by the ministry directors or supervising adults. Additionally, further research should be done as to objectionable content on trusted sites.
- 5. Ensure that movie viewing is always in compliance with appropriate copyright and licensing laws.

Computers and Internet:

In using a computer, the internet, or any electronic device provided by the Eparchy or any of its entities, employees and volunteers must:

- 1. Respect other's privacy.
- 2. Password protect all computers and devices used for ministry purposes.
- 3. Safeguard user IDs and passwords.
- 4. Always log off the system before walking away from the computer or use a password protected screen saver.
- 5. Honour copyright and licence agreements.
- 6. Protect confidential information from unauthorized use or disclosure.
- 7. Never use these electronic devices or the internet for illegal purposes in violation of any international, federal, provincial, or local laws.
- 8. Never attempt to bypass, block, or remove filtering software.
- 9. Not conceal activities that are otherwise in violation of acceptable use of technology according to the Eparchial policy. Utilizing tools such as incognito or private mode to prevent any sort of monitoring or detection is forbidden. Do not use secretive or deceptive applications,
- 10. Scan for viruses when downloading files from the internet.