Министерство образования и науки Хабаровского края
краевое государственное казенное общеобразовательное учреждение
для детей-сирот и детей, оставшихся без попечения родителей, реализующее адаптированные основные общеобразовательные программы
«Школа-интернат № 4»

Принято с учетом мнения Совета школы
(протокол № 3 от «14» 06 2022)

ПРИНЯТО
Педагогическим Советом
Образовательного учреждения
протокол от «13» 06 2022 г. № 9
Председатель Совета _____ И.В. Жабицкая

УТВЕРЖДЕНО
приказ от «22» 06 2022 г. № 229
Директор _____ И.В. Жабицкая

ПОЛОЖЕНИЕ
о создании и ведении (наполнении) аккаунтов КГКОУ ШИ 4 в социальных сетях

Хабаровск, 2022

1. Общие положения

1.1. Настоящее положение разработано в соответствии с постановлением Правительства Хабаровского края от 17.03.2020 № 77-пр "О взаимодействии органов исполнительной власти Хабаровского края с населением Хабаровского края в информационно-телекоммуникационной сети "Интернет" в целях обеспечения защищенности аккаунтов в социальных сетях (далее – Аккаунты).

1.2. Настоящее Положение определяет правила создания и ведения (наполнения) аккаунтов КГКОУ ШИ 4 в социальных сетях в информационно-телекоммуникационной сети "Интернет","ВКонтакте", "Телеграмм" (далее - социальные интернет-сети).

1.3. Под аккаунтами КГКОУ ШИ, в социальных интернет-сетях в целях настоящего Положения понимается хранимая в социальных интернет-сетях совокупность данных об учреждении, необходимая для их опознавания (аутентификации) и предоставления доступа к работе в социальных интернет-сетях (далее - КГКОУ ШИ 4).

2. Осуществление создания и ведения (наполнения) аккаунтов школы-интерната

2.1. Ответственные лица за создание и ведение (наполнение) аккаунтов КГКОУ ШИ 4 назначаются директором учреждения и осуществляют:

2.2. Создание и ведение (наполнение) аккаунтов школы-интерната, модерирование комментариев и сообщений в них.

2.3. Работу по обеспечению защищенности аккаунтов министерства (принятие мер, направленных на обеспечение безопасности данных и на защиту аккаунта от несанкционированного доступа).

2.4. Ведение КГКОУ ШИ 4 на основании подготовленного графика выхода и содержания публикаций (контент-плана) о мероприятиях и других информационных поводов, связанных с деятельностью школы-интерната.

3. Ведение (наполнение) аккаунтов КГКОУ ШИ 4

3.1. В аккаунтах школы-интерната размещается информация о деятельности, другая общественно значимая для учреждения информация, связанная с деятельностью школы.

3.2. При ведении аккаунтов КГКОУ ШИ 4 используются тексты, фотографии, инфографика, карточки, анимация, видео, опросы, конкурсы, акции, иные материалы и форматы с учетом специфики каждой социальной интернет-сети.

2.3. Аккаунты школы должны иметь текстовое описание и дизайнерское оформление.

2.4. При написании текстов публикаций в аккаунтах используется стиль общения, характерный для данной социальной интернет-сети (письменная разговорная речь).

2.5. Удалению из аккаунтов школы-интерната подлежат комментарии и сообщения, нарушающие положения действующего законодательства Российской Федерации. Также подлежат удалению комментарии, содержащие рекламные рассылки, оскорбления и нецензурные выражения. При этом пользователям, допустившим такие комментарии и сообщения, могут быть ограничены коммуникативные возможности, предоставляемые социальными интернет-сетями, в рамках аккаунтов.

4. Меры по защите автоматизированных рабочих мест, с которых осуществляется работа в Аккаунтах

4.1. Требования к автоматизированным рабочим местам (далее – АРМ) при ведении Аккаунтов:

– на АРМ должно быть установлено лицензионное общесистемное и прикладное программное обеспечение (операционная система, интернет браузер и т.п.), а также выполнено обновление до актуальных версий, имеющих действующую техническую поддержку производителя;

– на АРМ должно быть установлено лицензионное антивирусное программное обеспечение (далее – ПО) с включением максимально возможного количества модулей защиты (межсетевой экран, система обнаружения вторжений, блокирование вредоносного ПО и других угроз, защита от сбора данных, обнаружение шпионского ПО и т.д.) и максимально возможного уровня защиты, с актуальными антивирусными базами;

– на АРМ необходимо настроить блокировку экрана при превышении определенного времени неиспользования АРМ (рекомендованное время простоя не более 5 минут).

4.2. Количество рабочих мест должно быть сведено к минимуму.

4.3. Рекомендуется не осуществлять работу в социальных сетях с мобильных устройств (мобильные телефоны, планшеты).

4.4. При необходимости осуществления доступа в социальные сети с мобильного устройства требуется исключить использование общедоступных Wi-Fi сетей, в связи с большой возможностью перехвата учетных данных владельцем Wi-Fi точки доступа.

5. Меры защиты при работе в Аккаунтах

5.1. Настройки безопасности Аккаунтов[1]:

– обеспечить включение привязки номера телефона и дополнительного адреса электронной почты к Аккаунтам;

– обеспечить включение двухфакторной аутентификации – по логину, паролю и по СМС сообщению на телефон;

– использовать надежный пароль для каждого Аккаунта:

[1] Устанавливаются при наличии технической возможности в аккаунте социальной сети.

а) пароль должен содержать не менее восьми символов;

б) пароль должен содержать символы верхнего и нижнего регистров;

в) пароль должен содержать комбинации букв и цифр, по возможности – спецсимволы (!@#$%^&);

г) пароль не должен нести смысловой нагрузки, в качестве пароля не рекомендуется использовать часто употребляемые слова;

д) использовать уникальные пароли для различных Аккаунтов;

е) не использовать для записи паролей: стикеры, блокноты, а также иные способы, не обеспечивающие сохранение их в тайне;

ж) пароль рекомендуется периодически изменять (один раз в 3 месяца).

В случае подозрения на компрометацию пароля или увольнения/изменения ответственного лица за ведение Аккаунтов необходимо изменить пароль и данные для восстановления доступа к Аккаунтам;

– необходимо хранить данные о восстановлении доступа к Аккаунтам в актуальном состоянии и в надежном месте (например, в личном сейфе).

5.2. При авторизации в Аккаунтах необходимо проверять подлинность адреса страницы в сети "Интернет" и наличие актуального сертификата. При отсутствии сертификата вводить логин и пароль запрещается.

5.3. По завершению работы в социальных сетях осуществлять выход из Аккаунтов.

5.5. При работе на АРМ в сети "Интернет" необходимо соблюдать общие правила, в том числе:

– не скачивать и не запускать подозрительные файлы;

– не переходить по подозрительным ссылкам, в том числе размещенным в комментариях;

– не посещать подозрительные ресурсы, сайты с ошибками или с отсутствующими сертификатами, вводить на данных сайтах логины и пароли.

5.6. При работе на АРМ с электронной почтой необходимо проверять полученные письма на "спам", а также на наличие вложений и ссылок. При наличии вложений удостовериться, действительно ли письмо предназначается школе-интернату. В случае возникновения подозрений уточнить у отправителя по иному каналу связи, не обозначенному в письме (например, телефон), о направлении в адрес школы письма с вложением. Вложение всегда размещается под полем "Кому".

При наличии в письме ссылок, картинок, кнопок и т.д. запрещается нажимать на данные "активные" элементы, что может повлечь переход на зараженные вирусом веб-ресурсы в сети "Интернет" или скачивание файлов, зараженных вирусами. При необходимости перехода на указанные в письме ресурсы рекомендуется адрес ресурса самостоятельно вводить в адресную строку браузера.

При получении писем о блокировке, подозрении на взлом, взломе Аккаунтов, необходимости изменения паролей или другой учетной информации запрещается переходить по ссылкам, указанным в письме.

Для проверки доступности Аккаунта необходимо самостоятельно ввести в адресную строку браузера адрес ресурса, о котором сообщено в

письме и удостоверится в доступности Аккаунта. При необходимости сменить пароль.