Муниципальное общеобразовательное учреждение лицей № 2

СОГЛАСОВАНО
Педагогическим советом
лицея № 2
(протокол от 02.11.2022 № 3)

УТВЕРЖДЕНО
приказом лицея № 2
от 07.12.2022 № 536
Директор
П.Е. Щедрина

Порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным методическим материалам, музейным фондам, материально-техническим средствам обеспечения образовательной деятельности

1. Настоящий Порядок регламентирует доступ педагогических работников муниципального общеобразовательного учреждения лицея № 2 (далее — лицей) к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, музейным фондам, материально-техническим средствам обеспечения образовательной деятельности.

2. Доступ педагогических работников к вышеперечисленным ресурсам осуществляется с учетом базовые требований соблюдения информационной безопасности на рабочих местах (Приложение 1) и обеспечивается в целях качественного осуществления образовательной и иной деятельности, предусмотренной уставом лицея.

3. Доступ к информационно-телекоммуникационным сетям.

3.1. Доступ педагогических работников к информационно- телекоммуникационной сети Интернет в лицее осуществляется с персональных компьютеров (ноутбуков, планшетных компьютеров и т.п.), подключенных к сети Интернет, без ограничения времени и потребленного трафика.

3.2. Доступ педагогических работников к локальной сети лицея осуществляется с персональных компьютеров (ноутбуков, планшетных компьютеров и т.п.), подключенных к локальной сети лицея, без ограничения времени и потребленного трафика.

3.3. Для доступа к информационно-телекоммуникационным сетям в лицее педагогическому работнику предоставляются идентификационные данные (логин и пароль / учётная запись / электронный ключ и др.). Предоставление доступа осуществляется работником, назначенным ответственным за информационную безопасность лицея № 2.

4. Доступ к базам данных

4.1. Педагогическим работникам обеспечивается доступ к следующим электронным базам данных:

- профессиональные базы данных;
- информационные справочные системы;
- другие по мере появления.

4.2. Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных лицеем с правообладателем электронных ресурсов (внешние базы данных).

4.3. Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте лицея в разделе «Информационные ресурсы». В данном разделе описаны условия и порядок доступа к каждому отдельному электронному ресурсу.

5. Доступ к учебным и методическим материалам

5.1. Учебные и методические материалы, размещенные на официальном сайте лицея, находятся в открытом доступе.

5.2. Педагогическим работникам по их запросам могут выдаваться во временное пользование учебные и методические материалы, входящие в оснащение учебных кабинетов.

Выдача педагогическим работникам во временное пользование учебных и методических материалов, входящих в оснащение учебных кабинетов, осуществляется работником, на которого возложено заведование учебным кабинетом.

Срок, на который выдаются учебные и методические материалы, определяется работником, на которого возложено заведование учебным кабинетом, с учетом графика использования запрашиваемых материалов в данном кабинете.

Выдача педагогическому работнику и сдача учебных и методических материалов фиксируется в журнале выдачи.

При получении учебных и методических материалов на электронных носителях, подлежащих возврату, педагогическим работникам не разрешается стирать или менять на них информацию.

6. Доступ к фондам музея лицея.

Доступ педагогических работников, а также организованных групп обучающихся под руководством педагогического работника (работников) к фондам музея Учреждения осуществляется бесплатно.

Посещение музея лицея организованными группами обучающихся под руководством педагогических работников осуществляется по согласованию с заместителем директора по воспитательной работе.

7. Доступ к материально-техническим средствам обеспечения образовательной деятельности.

7.1. Доступ педагогических работников к материально-техническим средствам обеспечения образовательной деятельности осуществляется:

– без ограничения к учебным кабинетам, лабораториям, мастерским, спортивному и актовому залам и иным помещениям и местам проведения занятий во время, определенное в расписании занятий;

– к учебным кабинетам, лабораториям, мастерским, спортивному и актовому залам иным помещениям и местам проведения занятий вне времени, определенного расписанием занятий, по согласованию с работником, ответственным за данное помещение.

7.2 Использование движимых (переносных) материально-технических средств обеспечения образовательной деятельности (проекторы и т.п.) осуществляется по письменной заявке, поданной педагогическим работником (не менее чем за 2 рабочих дня до использования материально-технических средств) на имя лица, ответственного за сохранность и правильное использование соответствующих средств.

Выдача педагогическому работнику и сдача им движимых (переносных) материально-технических средств обеспечения образовательной деятельности

фиксируются в журнале выдачи.

7.3 Для копирования или тиражирования учебных и методических материалов педагогические работники имеют право пользоваться копировальным автоматом.

7.4. Для распечатывания учебных и методических материалов педагогические работники имеют право пользоваться принтером.

7.5. В случае необходимости тиражирования или печати сверх установленного объёма педагогический работник обязан обратиться со служебной запиской на имя директора лицея.

8. Накопители информации (CD-диски, флеш-накопители, карты памяти), используемые педагогическими работниками при работе с компьютерной информацией, предварительно должны быть проверены на отсутствие вредоносных компьютерных программ.

Приложение 1

Базовые требования соблюдения информационной безопасности на рабочих местах

Доступ к ресурсам и сервисам, обеспечивающим функции образовательной организации

1. Использовать только сложные пароли: они должны быть не менее 12 знаков длиной, не состоять из словарных слов, содержать спецсимволы и цифры. Если пароль простой, злоумышленник удаленно с помощью специальных программ сможет подобрать его простым перебором.

2. Пароли должны быть уникальными: не используйте один и тот же пароль для всех рабочих ресурсов. Тем более — не используйте его же и в личных целях. Достаточно будет утечки из одного из сервисов, чтобы скомпрометировать в этом случае доступ ко всем ресурсам.

3. Пароли должны быть секретными: не записывайте пароль на бумаге и не храните около рабочего места; не вписывайте их в файлы и не делитесь ими с коллегами. Иначе случайный посетитель или уволившийся сотрудник сможет воспользоваться таким паролем.

4. Включить, двухфакторную аутентификацию, если сервис позволяет ее включить. Это не позволит злоумышленнику получить доступ к сервису даже в случае утечки пароля.

О важности персональных данных

1. Не передавать файлы с персональными данными по электронной почте или по открытым каналам (например, через Google Docs по прямой ссылке или через публичные файлохранилища).

2. Не делится персональными данными, к которым Вы по своим обязанностям имеете доступ, с коллегами, чьи рабочие функции не требуют такого доступа, с посторонними лицами, с обучающимися.

О самых распространенных киберугрозах

1. Тщательно проверять ссылки в письмах, прежде чем по ним переходить. Убедительно выглядящее имя отправителя — не гарантия подлинности. Злоумышленники могут попробовать подсунуть фишинговую ссылку, особенно если им удастся захватить почту кого-то из ваших коллег.

2. Убедитесь, что на всех рабочих компьютерах подключена автоматическая проверка антивирусом при подключении USB устройств (флеш-накопители, карты памяти, переносные жесткие диски, телефоны сотрудников через USB) . При настройке антивируса установите отключение автозапуска любой информации с подключаемых через USB устройств. Не подключайте к рабочему компьютеру любые сторонние флеш носители.

3. Не открывайте и не запускайте любые файлы из непроверенного источника (например, присланные по почте). При открытии файла всегда нужно смотреть, не является ли он исполняемым (злоумышленники часто маскируют вредоносные файлы под офисные документы). Любой присланный по почте файл необходимо сначала сохранить в папку, выделенную на локальном компьютере для файлов, которые не проверены антивирусом, затем, не открывая его, запустить проверку на вирусы в этом файле.

Ссылки на полезные ресурсы

1. Инструкция по информационной безопасности для новых сотрудников https://www.kaspersky.ru/blog/security-awareness-basic-instruction/30980/

2. Как создавать сложные пароли https://www.kaspersky.ru/blog/use-strong-passwords/22732/

3. Почему нельзя использовать один и тот же пароль для нескольких сервисов https://www.kaspersky.ru/blog/never-reuse-passwords-story/21823/

4. Что такое BEC-атака и как ей противостоять (методы получения доступа к электронной почте сотрудников организации, основанные на технологических и социальных методов мошенничества) https://www.kaspersky.ru/blog/what-is-bec-attack/27623/