РЕКОМЕНДАЦІЇ ДЛЯ ПЕДАГОГІВ

Дотримуйтеся цих правил самі й розкажіть учням:

1. **Переконайтеся, що всі пристрої надійно захищені (паролями) і заблоковані тоді, коли ви ними не користуєтесь.** Якщо вам потрібно вийти з класу, заблокуйте всі пристрої, які використовували, або завершіть сеанс роботи чи вийдіть з облікового запису. Встановіть на всіх пристроях ліцензійну антивірусну програму та стежте за тим, щоби вона регулярно оновлювалася.
2. **Встановіть правила в школі, де й коли можна користуватися мобільними пристроями.** А також правила, що учнів можна фотографувати лише після отримання згоди батьків / опікунів / самих учнів на це. Ці правила мають бути закріплені в шкільній політиці щодо онлайн-безпеки. Така політика має встановлювати ще й порядок реагування на інциденти, пов'язані з безпекою дітей, зокрема, у цифровому середовищі. Так, у школі може бути призначений спеціальний координатор для обліку та реєстрації порушень та інцидентів, пов'язаних з онлайн-безпекою, задля формування цілісного уявлення про наявні в школі проблеми та тенденції, що вимагають уваги.
3. **Забезпечте фільтрацію й моніторинг даних, які передаються через шкільну мережу, встановивши необхідні програми.** Допомогти їх встановити можуть інтернет-провайдери. Учні не повинні отримувати доступу до шкідливого або неприйнятного контенту через шкільну мережу. Такі системи фільтрації та контролю контенту допомагають звести до мінімуму передавання неприйнятного (наприклад, насильницького чи порнографічного) контенту в шкільній мережі. А системи фільтрації даних допомагають відстежувати, хто, що, коли й на якому пристрої завантажує. Такий механізм є одним зі способів запобігання кібербулінгу.
4. **Пам'ятайте, що ваші дії та слова в інтернеті можуть вплинути на вашу онлайн-репутацію, а також на репутацію навчального закладу.** Ви як користувач/-ка інтернету залишаєте свій цифровий слід – адже різні сайти, соціальні мережі, платформи, відповідно до своїх політик, збирають дані про вашу онлайн-активність. Перевіряйте інформацію, яку поширюєте в соціальних мережах. Перед тим як опублікувати інформацію, подумайте, хто може її побачити. Розповідайте дітям про важливість онлайн-репутації та як правильно її формувати.
5. **Слідкуйте за своєю професійною комунікацією**. Для будь-яких контактів між працівниками школи, учнями, батьками чи іншими зацікавленими сторонами завжди використовуйте шкільну електронну пошту замість особистої. У деяких випадках кодекс ділової етики, якщо він погоджений у школі, може передбачати заборону на контакти з учнями на платформах, які не мають стосунку до школи. Наприклад, у месенджерах чи соцмережах. Також рекомендується встановити в школі чіткі правила – як для працівників, так і для учнів – щодо проведення відеоконференцій чи занять у віддаленому режимі. Наприклад, правила, який вигляд має мати місце для проведення уроків, наявність фото профіля тощо.

6. **Сприяйте формуванню цифрових навичок та цифрової грамотності дітей.** Говоріть із ними про це на уроках. Намагайтеся включити до навчальних планів аспекти цифрової грамотності. Проводьте заходи в школі про онлайн-безпеку дітей. Водночас, показуйте високий рівень власної цифрової компетентності. І не забувайте проводити регулярну перевірку всіх заходів у школі на дотримання онлайн-безпеки дітей та її можливого удосконалення.
7. **Навчайтеся нового та постійно покращуйте навички цифрової грамотності**. Будьте в курсі того, які ризики на дітей можуть чекати в інтернеті, як діти проводять свій час у мережах. Це допоможе вам краще зрозуміти дітей та встановити з ними довірливі взаємини швидше й легше.

   Пам’ятайте, що **інтернет – одночасно й ризик, і можливість для дітей**. Тому освітянам варто робити все можливе, щоби зробити цифрове освітнє середовище максимально безпечним для дітей.