# Захист персональних даних під час дистанційного навчання

*Служба освітнього омбудсмена підготувала поради для педагогів, батьків та учнів про те, як захистити персональні дані під час дистанційного навчання.*

## Персональні дані та дистанційне навчання

В Україні поки ще немає чітко визначеної нормативної бази, яка б регулювала безпеку роботи вчителів та учнів в інтернеті під час дистанційного навчання, у тому числі безпеку роботи з персональними даними. Але ніщо не заважає нам використовувати на практиці ті норми законодавства, які ми вже маємо.

Положення про дистанційну форму здобуття повної загальної середньої освіти визначає, що під час дистанційного навчання освітній процес організовується з дотриманням вимог законодавства про захист персональних даних (частина 9 Положення).

А у листі МОН №1/9-609 від 02.11.20 року «Щодо організації дистанційного навчання» наголошується, що всі учасники освітнього процесу мають дотримуватися вимог щодо захисту персональних даних учасників освітнього процесу в електронному освітньому середовищі.

Основним законом із питання захисту персональних даних в нашій державі є Закон України «Про захист персональних даних», і саме його потрібно брати за основу для роботи з персональними даними та їхнього захисту.

Громадська організація Мінзмін за підтримки Міжнародного союзу електрозв'язку (МСЕ) та за ініціативи Міністерства цифрової трансформації України переклала

**«Загальні рекомендації щодо захисту дітей у цифровому середовищі».**

## Що робити закладам освіти задля безпеки дистанційного навчання

Міжнародний союз електрозв'язку визначає наступні рекомендації для закладів освіти.

**Заклад освіти має:**

- забезпечити захищену та надійну шкільну мережу, а для цього потрібно використовувати послуги офіційного інтернет-провайдера. Під час дистанційного навчання вчителі та учні використовують особисті домашні пристрої, які зазвичай не охоплюються мережевим захистом. У такому випадку вчителям та батькам учнів варто перевірити офіційність та надійність свого інтернет-провайдера, щоб оцінити можливі ризики. Якщо провайдер неофіційний — посилити захист за допомогою програмного забезпечення. Також ключове значення мають проведення для учнів навчання про безпеку в інтернеті, обговорення різних практичних випадків та діалог;
- використовувати програмне забезпечення для фільтрації та моніторингу безпеки пристроїв;
- встановлювати політику в межах школи, що регулює, де і як можуть використовувати технології різні учасники навчального процесу, а також порядок реагування на інциденти, пов’язані з безпекою дітей, зокрема, у цифровому середовищі;
- організовувати для учнів навчання з питань онлайнової безпеки;
- забезпечувати достатній рівень підготовки всіх співробітників (зокрема, технічного персоналу), а також регулярне підвищення їхньої кваліфікації;
- призначити у школі спеціального координатора і створити можливості для обліку та реєстрації інцидентів, пов’язаних з онлайновою безпекою, щоб сформувати цілісне уявлення про наявні у школі проблеми та тенденції, що вимагають уваги;
- вжити заходів для того, щоб адміністративно-управлінський персонал та керівники були достатньо обізнані в питаннях онлайнової безпеки у школі;

- взяти до уваги потенційний вплив інтернету та онлайнових технологій на навчання та психіку учнів.

Відповідно до Положення про дистанційну форму здобуття повної загальної середньої освіти, електронні освітні платформи, онлайн сервіси та інструменти, за допомогою яких організовується освітній процес під час дистанційного навчання, обирає та схвалює педагогічна рада закладу освіти (частина 5, розділ І Положення).

Ми вже наголошували на тому, що рекомендуємо педагогам обирати для дистанційного навчання одну або дві освітні платформи, оскільки це полегшить учням, учителям та батькам організацію навчання. Також використання мінімальної можливої для забезпечення освітнього процесу кількості платформ робить дистанційне навчання безпечнішим, оскільки зменшується ризик витоку персональних даних. Як у випадку з провайдером, рекомендуємо обирати перевірені платформи від офіційних виробників та не надавати зайвих персональних даних учнів і вчителів для користування платформами. Заклад освіти має повідомити учнів та батьків, які персональні дані будуть оброблятися під час використання тієї чи іншої платформи дистанційного навчання.

Водночас радимо закладам освіти звернути увагу на розробку певних правил поведінки та безпеки в онлайн середовищі і порядок реагування на інциденти. Спільне обговорення та прийняття цих правил з учнями та батьками дозволить мінімізувати неприємні випадки, які періодично трапляються під час дистанційного навчання.

**Що робити педагогічним працівникам для безпеки дистанційного навчання**

Міжнародний союз електрозв’язку визначає такі **рекомендації для вчителів.**

Насамперед необхідно слідкувати за безпекою та надійністю як домашніх, так і робочих пристроїв, які ви використовуєте для проведення дистанційного навчання. Для цього:

- переконайтеся в тому, що всі пристрої надійно захищені та на них встановлено пароль. Учителі настільки ж вразливі перед кібератаками, шкідливими програмами, вірусами та зламами, як і всі інші. Важливо, щоб усі пристрої, які ви використовуєте, захищалися надійним паролем. Як створити надійний пароль і не забути його, можна прочитати тут;
- блокуйте пристрої, завершуйте сеанс і виходьте з облікового запису, коли не використовуєте їх (наприклад, якщо виходите з кімнати або класу);
- встановіть антивірусне програмне забезпечення та брандмауер і регулярно їх оновлюйте.

Також дотримуйтеся визначеної закладом освіти політики щодо використання мобільних технологій та інших електронних пристроїв. Важливо, щоб при використанні пристроїв ви подавали учням приклад правильної поведінки.

Забезпечте фільтрацію та моніторинг даних, що передаються через шкільне під'єднання до інтернету (під час дистанційного навчання вдома – через домашнє під'єднання до інтернету). Учні не повинні отримувати доступу до шкідливого або неприйнятного контенту через шкільні ІТ-системи або ваше домашнє технічне обладнання. Системи фільтрації мають щонайменше блокувати доступ до незаконного контенту, а також контенту, який вважається неприйнятним або шкідливим.

Пам'ятайте про власну онлайн-репутацію та цифровий слід, який залишаєте, про те, що ваші слова та дії в інтернеті можуть вплинути як на вашу власну репутацію, так і на репутацію закладу освіти. Також розповідайте дітям про важливість онлайнової репутації й про те, як правильно її формувати.

Між приватним та професійним життям учителів завжди має бути чітка межа, зокрема, й у цифровому середовищі. Для будь-яких контактів між співробітниками школи та учнями або батьками завжди необхідно використовувати шкільну електронну пошту. Шкільна комунікаційна політика може забороняти будь-які контакти, не пов'язані з освітньою діяльністю, та контакти на платформах, що не мають стосунку до школи.

На випадок проведення відеоконференцій або занять у віддаленому режимі, школи мають установлювати чіткі приписи як для співробітників, так і для учнів (наприклад, що бажано підготувати місце для віддаленого заняття/сеансу зв'язку та подбати про тих, хто перебуває поруч – чи то вдома, чи то в класі).

Учителі мають розуміти, чим інтернет може бути для учнів небезпечний і чим корисний. Докладні рекомендації тут.
Для безпеки педагогів радимо також створити окремий обліковий запис або окремого користувача, якщо ділите вдома чи на роботі свій пристрій ще з кимось, і також розмежувати ваші власні електронні скриньки для особистого користування та для робочих питань.

Звертаємо вашу увагу на пересилання персональної інформації (власної або учня) через соціальні мережі, різноманітні месенджери, електронною поштою. Поміркуйте, чи конче необхідно надсилати персональні дані у повідомленні. Якщо це все ж необхідно, ретельно перевірте, чи правильно ви вказали адресата.

**Поради для батьків**

Захист персональних даних – це спільна робота педагогів, батьків та учнів. Тому чималу роль у тому, чи буде дистанційне навчання успішним, якісним та безпечним для дитини, відіграють батьки. Просимо вас розповісти дітям про персональні дані, про небезпеку їхнього поширення і правила поводження з ними.

Для батьків Міжнародний союз електрозв'язку визначає такі рекомендації.

- Насамперед спілкуйтеся зі своїми дітьми, цікавтеся, що вони люблять переглядати в інтернеті, спробуйте організувати спільно з ними будь-яку онлайнову діяльність.
- Визначте, які технології, пристрої та послуги використовуються у вас вдома.
- Встановіть на всіх пристроях брандмауер та антивірусну програму. Поміркуйте над тим, чи будуть корисними та чи підходять для вашої родини програми фільтрації, блокування або відстеження. Розгляньте можливість використання контент-фільтрів, що досить часто називаються системами батьківського контролю, і безпечних пошукових систем або обмежень доступу, щоб фільтрувати контент, який діти можуть переглядати в інтернеті.
- У колі родини домовтеся про умови використання інтернету й особистих пристроїв, приділяючи особливу увагу питанням конфіденційності, вікової відповідності змісту сайтів, додатків та ігор, булінгу, кількості проведеного перед екраном часу та небезпеки з боку незнайомців.
- Поясніть дітям, що перш ніж публікувати світлини або відео в мережі, слід отримати згоду людей, які там зображені. Батькам також варто звертати увагу на те, якою інформацією про своїх дітей вони діляться в соціальних мережах і в інтернеті загалом, зокрема, це стосується особистих історій про дітей або їхніх світлин. Пам'ятайте про недоторканність приватного життя вашої дитини!
- Поясніть дітям, що не можна повідомляти свої паролі доступу друзям або братам і сестрам. Звертайте їхню увагу на те, коли і де вони повідомляють свою персональну інформацію – наприклад, навчайте, що в загальнодоступному профілі краще використовувати деперсоніфіковані зображення як фотографії профілю і вказувати мінімум персональної інформації, такої як вік, школа та місце проживання.

- Зверніть увагу на вік «цифрової згоди». У деяких країнах діють закони, що встановлюють мінімальний вік, починаючи з якого компанії або вебсайти можуть просити дітей повідомити персональну інформацію без попереднього отримання підтвердженої згоди батьків. Вік «цифрової згоди» зазвичай варіюється в межах 13–16 років. На багатьох вебсайтах, призначених для дітей молодшого віку, потрібна згода батьків для реєстрації нового користувача.
- Дізнайтеся, як повідомити про проблему на платформах, якими користуються ваші діти, і як видалити профіль або змінити зазначену в ньому інформацію.
- Розкажіть про важливість персональної інформації. Поясніть дітям, що їм слід ділитися тільки тією інформацією, яку, на вашу і на їхню думку, дозволено побачити стороннім. Їм не слід ділитися інформацією, що дозволяє встановити їхню особистість або особистість інших. Нагадайте дітям, що в них є онлайн репутація, за якою необхідно стежити, а після того, як контент опубліковано, його може бути складно змінити або скорегувати.
- Переконайтеся, що діти розуміють, що означає публікація світлин та відео в інтернеті, у тому числі їхніх власних та їхніх друзів. Поясніть дітям, що фотографії та відео можуть розкривати безліч персональної інформації. Діти повинні розуміти ризики, пов’язані з використанням камер та опублікуванням контенту. Бажано, щоб світлини інших людей не викладалися без їхньої згоди. Це також стосується і батьків, які роблять та публікують знімки своїх дітей. Крім того, важливо, щоб діти розуміли, що іноді інформацію може розкрити хтось із їхніх друзів або членів сім’ї, тому їм варто поговорити про це зі своїми друзями та родичами і розповісти про небезпеку надмірного розкриття інформації. Порадьте своїм дітям не викладати власні фото та відео або фото та відео друзів, на яких є елементи, що легко піддаються ідентифікації, наприклад, таблички з назвами вулиць, автомобільні номери або назва школи на толстовках тощо.

Звертаємося до всіх учасників освітнього процесу: з повагою ставтеся один до одного, адже безпека як очного, так і дистанційного навчання залежить від педагогів, батьків, учнів та студентів.

***За матеріалами Офісу освітнього омбудсмена.***