ЗАКЛАД ДОШКІЛЬНОЇ ОСВІТИ (ясла-садок) №219 «СОНЯЧНИЙ ЗАЙЧИК ЗАПОРІЗЬКОЇ МІСЬКОЇ РАДИ

ПОГОДЖЕНО
Профспілковий комітет ЗДО №219
протокол від 30.08.2023 № 09
Голова ПК _____
Любов КОНОНЕНКО

СХВАЛЕНО
на засіданні педради ЗДО №219
протокол від 30.08.2023 №01

ЗАТВЕРДЖЕНО
наказом від 31.08.2023 № 042/р
Директор _____ Лідія ЯСИР

ПОЛОЖЕННЯ

Про цифрову безпеку закладу освіти

Заклад дошкільної освіти (ясла-садок) №219

«Сонячний зайчик»

Запорізької міської ради

м. Запоріжжя

2023

Зміст

I РОЗДІЛ. Загальні положення 3

II РОЗДІЛ. Системотехнічне забезпечення цифрового освітнього простору закладу освіти 5

III РОЗДІЛ. Електронне діловодство закладу освіти.....8

IV РОЗДІЛ. Сайт закладу освіти.....9

Інформаційне наповнення сайту формується відповідно до вимог чинного законодавства, зокрема, відповідно до ст. 30 Закону України «Про освіту», та статутної діяльності закладу з суспільно-значущої інформації як для всіх учасників освітнього процесу, так і для інших зацікавлених осіб. 10

V РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (ел. пошта закладу освіти).....12

VI РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (соціальні мережі, месенджери).....14

VII РОЗДІЛ. Особливості провадження освіти, дистанційної освіти.....17

Організація освітнього процесу. Особливості дистанційної освіти 17

VIII РОЗДІЛ. Проведення заходів просвітницького характеру 18

IX РОЗДІЛ. Захист персональних даних в цифровому середовищі закладу освіти.....25

X РОЗДІЛ. Прикінцеві положення 26

Використані джерела: 27

ПОЛОЖЕННЯ

Про цифрову безпеку закладу освіти

І РОЗДІЛ. Загальні положення

Положення «Про цифрову безпеку закладу освіти» визначає політику цифрово безпеки закладу дошкільної освіти (ясел-садка) №219 «Сонячний зайчик» Запорізько міської ради (далі – ЗДО №219).

Положення «Про цифрову безпеку закладу освіти» (далі – Положення) опису основні принципи побудови системи управління інформаційною безпекою заклад освіти, посадових обов'язків і практик, які використовуються закладом освіти дл зменшення цифрових ризиків та збереження персональних даних учасників освітнього процесу.

Положення розроблене з урахуванням вимог законів України «Про освіту», «Пр повну загальну середню освіту», «Про дошкільну освіту», «Про позашкільну освіту законів України, дія яких поширюється на впровадження та використан інформаційних технологій у сфері освіти в Україні: «Про інформацію», «Про досту до публічної інформації», «Про захист персональних даних», «Про Національ програму інформатизації», «Про захист інформації в інформаційн телекомунікаційних системах», «Про електронні комунікації», «Про основні заса забезпечення кібербезпеки України», «Про електронні документи та електронн документообіг».

Реалізація безпекової політики в закладі освіти та забезпечення розвит інформаційно-комунікаційних технологій, зокрема, в сфері освіти, здійснюєть відповідно до положень Стратегії розвитку інформаційного суспільства в Украї схваленої розпорядженням Кабінету Міністрів України від 15.05.2013 № 386 Стратегії інформаційної безпеки на період до 2025 року, затвердженої указ Президента України від 28.12.2021 № 685/2021, Стратегії кібербезпеки Україн затвердженої указом Президента України від 26.08.2021 № 447/2021, Концеп розвитку цифрових компетентностей, схваленої розпорядженням Кабінету Міністр України від 03.03.2021 № 167-р.

У Положення нижченаведені терміни вживаються в такому значенні:

база персональних даних - іменована сукупність упорядкованих персональн даних в електронній формі та/або у формі картотек персональних даних;

безпека мережі - здатність електронних комунікаційних мереж протистояти дія що становлять загрозу доступності, цілісності чи конфіденційності таких мереж також даних, що зберігаються, передаються чи обробляються;

гаджет – пристрій, пристосування, яке виконує обмежене коло завдань;

дані - інформація, яка подана у формі, придатній для її оброблення електронни засобами;

документ - матеріальний носій, що містить інформацію, основними функція якого є її збереження та передавання у часі та просторі;

девайс – пристрій, пристосування, створене людиною для вирішення широко кола завдань, комп'ютерна техніка та електроніка;

електронні інформаційні ресурси - систематизовані відомості і дані, створе оброблені та збережені в електронній формі за допомогою технічних засобів та/а програмних продуктів;

засоби інформатизації - комп'ютери, програмні продукти, інформаційні системи або їх окремі елементи, електронні комунікаційні мережі, що використовуються для реалізації інформаційно-комунікаційних технологій;

захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформатизація - сукупність взаємопов'язаних організаційних, правових, технологічних, виробничих інших процесів, спрямованих на створення умов для забезпечення розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій;

інформаційно-комунікаційні технології - результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг;

інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

інформаційна діяльність - це створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації;

комунікація - це процес спілкування і передачі інформації між людьми або їх групами у вигляді усних і письмових повідомлень;

месенджер – телекомунікаційна служба для обміну текстовими повідомленнями між комп'ютерами або іншими пристроями користувачів через комп'ютерні мережі;

мобільний пристрій – це загальний термін для будь-якого портативного комп'ютера або смартфон;

оцифрування - це створення цифрового зображення фізичних об'єктів або атрибутів; в рамках оцифрування не відбувається змін структури інформації, вона просто набуває електронну форму для подальшої обробки в цифровому форматі;

персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

соціальна мережа – соціальна структура, утворена індивідами або організаціями, вебсайт або інша служба у Веб, яка дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок та переглядати власний список зв'язків і списки інших користувачів;

хмарні технології – це технології, які надають користувачам Інтернету доступ до комп'ютерних ресурсів сервера і використання програмного забезпечення як онлайн-сервіса;

цифрова компетентність – здатність використовувати цифрові медіа й електронні освітні ресурси (ЕОР), розуміти та критично оцінювати різні аспекти медіа - цифрових і контенту, а також якість, що вказує на рівень кваліфікації практичного використання ЕОР;

цифрова технологія - сукупність систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації;

цифровізація - процес впровадження цифрових технологій у всі сфери суспільного життя.

Інші терміни вживаються у даному Положенні у значеннях, визначе законодавчими актами України.

ІІ РОЗДІЛ. Системотехнічне забезпечення цифрового освітнього простору закладу освіти

Цифровий освітній простір закладу освіти складають наступні компоненти:

внутрішні: комп'ютери, цифрове діловодство;

зовнішні: ресурси дистанційної освіти, вебсайт закладу освіти, блоги працівни месенджери, соціальні мережі.

Забезпеченість робочими комп'ютерами

1. Загальна кількість персональних комп'ютерів в закладі освіти складає 4 (з в робочому стані - 4, не працюють - 0).

2. Із загальної кількості персональних комп'ютерів (в робочому стані) - 4:

- робочі місця з комп'ютером у кабінеті психолога складає 1, у кабінеті сес медичної старшої -1, у методичному кабінеті – 1
- портативних комп'ютерів – 1;
- планшетів - 0.

3. В користуванні адміністрації – 1 персональних комп'ютерів, 1 стаціонар комп'ютерів, 0 – портативних комп'ютерів.

4. В користуванні педагогічних працівників – 2 персональних комп'ютерів них 1 – стаціонарних, 1 – портативних, що складає 50% .

5. В користуванні адміністрації – всього 2 персональних комп'ютерів що скла 50% , із них 1 – стаціонарних комп'ютерів, 1– портативних.

6. Наявність комп'ютерної техніки, якій більше 5 років, складає 4 .

7. Кількість персональних комп'ютерів версії операційних систем – Windo (7,10,11) або Linux складає 4.

Налаштування та обслуговування комп'ютерів працівників

В закладі освіти призначається відповідальна особа (-и), яка (-і) виконує (-ю налаштування комп'ютерів працівників, включаючи адміністратора мережі.

Адміністратор мережі (інженер електронік, відповідальна особа) має(-ю знання про мережеві налаштування, установку програмного забезпечення та безпек відповідає за належне функціонування комп'ютерів у мережі.

У деяких випадках працівники можуть самостійно налаштовувати свої особи комп'ютери, особливо, якщо вони працюють з власних пристроїв.

Відповідальна особа закладу освіти надає настанови та рекомендації що необхідних налаштувань та доступів до мережі, але виконання цих налаштувань зоною відповідальності працівників (розробляються «Загальні настанови рекомендації щодо налаштувань і доступів до мережі»).

Щодо налаштування доступів, адміністратор мережі може керувати доступам до різних ресурсів, таких як файли, папки, програми або вебсайти, налаштовує пра доступу та ролі для кожного працівника.

Налаштування комп'ютерів працівників закладу освіти	ПІБ відповідальної особи

Адміністратор мережі (інженер електронік, відповідальна особа)	
Самостійне налаштування при роботі працівника на особистому комп'ютері. Обов'язкове ознайомлення працівників з «Загальними настановами та рекомендаціями щодо налаштувань і доступів до мережі»	

Загальні настанови та рекомендації щодо налаштувань і доступів до мережі:

1. Пароль і безпека:

Встановіть надійний пароль для вашого комп'ютера, мережевого обладнання та облікових записів.

Регулярно оновлюйте паролі і уникайте використання слабких або очевидних паролів.

Використовуйте двоетапну аутентифікацію, якщо це можливо, для додаткового рівня безпеки.

2. Оновлення програмного забезпечення:

Переконайтеся, що ваша операційна система та інші програми на комп'ютері оновлені до останніх версій.

Включіть автоматичне оновлення, щоб отримувати нові патчі і виправлення безпеки.

Захист від шкідливих програм.

3. Встановіть надійне антивірусне програмне забезпечення та антивірусні програми.

Регулярно скануйте свій комп'ютер на віруси та шкідливе ПЗ.

Уникайте відкриття підозрілих посилань або вкладень в електронних листах.

4. Налаштування мережі:

Встановіть пароль для вашої бездротової мережі Wi-Fi, щоб запобігти несанкціонованому підключенню.

Вимкніть безпроводове підключення (Wi-Fi) або від'єднуйте комп'ютер від мережі, якщо ви не використовуєте Інтернет.

5. Настройки файрволу:

Увімкніть файрвол (брандмауер) на комп'ютері для блокування небажаного мережевого трафіку.

Налаштуйте файрвол таким чином, щоб дозволити доступ лише до необхідних служб і портів.

6. Керування обліковими записами:

Створюйте окремі користувачів для кожного працівника та надавайте їм відповіді.

Ліцензійне програмне забезпечення

На комп'ютерні програми, які використовуються в закладі освіти, поширюється дія Закону України «Про авторське право і суміжні права», і їх використання можливе лише за умови дотримання вимог цього закону, а також вимог ліцензії, з якою користувач погоджується, установлюючи програму на свій комп'ютер.

У закладі використовується ліцензійне програмне забезпечення.

Порядок оновлення доступу при звільненні працівника

Для забезпечення цифрової безпеки в закладі освіти при звільненні праці виконуються наступні дії:

1. Працівник має перенести особисті та робочі файли з пристрою, наданого в користування, на особисті електронні носії.

2. Працівник має вийти з усіх облікових записів на пристроях, якими користується в закладі.

3. Працівник, що звільняється, має передати матеріальні цінності (прист надані йому в користування/наявні в кабінеті, завідувачу господарством уповноваженій особі.

4. Працівник, що звільняється, має видалитись з усіх корпоративних чатів, дію виконує адміністратор чатів *впродовж/не пізніше* наступних *5 днів* п звільнення працівника.

5. Уповноважена особа має оновити паролі до усіх інших облікових записів яких мав доступ працівник, що звільняється *впродовж/не пізніше* наступних 5 після звільнення працівника.

Збереження інформації

Для здійснення збереження та захисту даних закладу освіти керівник зак освіти призначає уповноважену ним особу (осіб), відповідальну за інформаці технічне забезпечення закладу освіти.

До функціональних обов'язків уповноваженої особи (осіб) вноситься запис:

Встановлення, збереження та оновлення паролів на всіх інформаційни технічних ресурсах освітнього закладу (адмінські паролі (сайт, база даних зак платформа для дистанційного навчання і т.п.)

При зміні технічного обладнання уповноважена особа (особи) контро технічні роботи, заміну та встановлення паролів.

Веде роз'яснювальну роботу серед учасників освітнього процесу необхідність цифрової безпеки у закладі.

Робота з паролями

При встановленні паролів уповноважена особа, працівники користую правилом складних паролів: пароль повинен містити 8 (12) і більше символів: ве та маленькі літери, цифри, спеціальні символи. Пароль має бути загальнодоступної інформації (ім'я, прізвище, нік, важливі дати, номери телеф ІПН, адреси і т.п.); для різних інформаційних ресурсів використовуються різні па

Для збереження паролів використовується:

- паперовий варіант – зберігається в сейфі адміністрації закладу;
- менеджер паролів – спеціальна програма, яка надає можливість тримати па у безпеці завдяки шифруванню. Потрібно пам'ятати один пароль для доступу до і бази (Google Password Manager, Bitwarden, LastPass, KeePass тощо).
- текстовий документ – зберігається документ в архіві під паролем;
- резервне копіювання для кожного способу.

Доступ до інформації та місця збереження паролів має предста адміністрації закладу освіти.

Обслуговування комп'ютерів, які використовуються для спільної роботи здійснюється уповноваженою відповідальною особою.

При наявності комп'ютерів для спільної роботи відповідальна особа має сприяти підвищенню безпеки і захисту робочого місця (персональних даних та комп'ютерних пристроїв):

1. Налаштувати захист. Доступ до груп налаштувати через корпоративні акаунти з будь-яких пристроїв.
2. Забезпечити коректне використання мережі Wi-Fi.
3. Прописати правила користування зовнішніми носіями інформації (флеш, карти пам'яті)
4. Слідкувати за оновленнями: переконатися, що отримуються автоматичні оновлення від служби Windows Update і інсталювати всі необхідні для організації оновлення.
5. Заборонити інсталювати програмне забезпечення з-поза меж організації, яке не затверджено або не адмініструється у закладі.
6. Безпечно зберігати дані. Заклад надає ресурс для зберігання даних, як-от GoogleDrive або інше корпоративне сховище. Не зберігати дані лише на локальному комп'ютері.
7. Постійно нагадувати (створювати пам'ятки, викладати їх на видне місце) щодо правил безпеки.

Функціонування загальної мережі ПК в закладі освіти

Персональні комп'ютери (ПК) в закладі освіти підключено до загальної мережі Інтернету.

Для підключення ПК до мережі укладено договір з інтернет-провайдером Linet, який забезпечує доступ до Інтернету через кабель.

Рівень доступу до мережі встановлюється шляхом налаштування мережевих параметрів на ПК.

На ПК встановлено тип підключення до мережі – бездротовий Wi-Fi (*або провідний Ethernet*), а також налаштовано доступ до мережі шляхом введення облікових даних (ім'я користувача та пароль).

Загальна мережа закладу освіти	
Інтернет провайдер закладу освіти	
Тип підключення закладу освіти до мережі Інтернету (бездротовий Wi-Fi або провідний Ethernet)	Провідний
Налаштування доступу до мережі Інтернету закладу освіти шляхом введення облікових даних, таких як ім'я користувача та пароль	Так

ІІІ РОЗДІЛ. Електронне діловодство закладу освіти

Ведення та зберігання ділової документації закладу освіти в електронній формі, спільна робота з електронними документами, обмін інформацією, як усередині

організації, так і в зовнішній її комунікації, здійснюється із застосуванням одн
хмарних рішень для роботи з документами *Google Drive* на платформі *Google*,
володіє та централізовано керує заклад освіти.

Найцінніші файли закладу зберігаються в хмарному сховищі, на спільних д
в домені закладу – https://drive.google.com/drive/u/0/my-drive. Власником файлів
зберігаються в хмарному середовищі закладу освіти, є заклад освіти, а не окр
працівник, який їх створює або додає. Заклад освіти є власником всього контенту
створюється та зберігається в межах платформи, у тому числі, після звільн
окремих працівників, які їх створювали або додавали.

До документів у хмарному сховищі надаються різні права доступу,
визначають певні можливості (редагування, коментування чи перегляд) та обмеж
відповідно до потреб закладу освіти.

Забороняється надання повного доступу за посиланням, для унеможливле
попадання посилань у відкритий доступ, що може призвести до безпек
інцидентів. Доступ надається конкретним людям суто із правами, які їм потрібні
виконання робочих завдань.

Контроль за виконанням електронних документів здійснює відповідальна ос
за діловодство у закладі освіти.

Контроль за виконанням електронних документів включає взяття електрон
документів на контроль, визначення форм і методів контролю, перевірку своєчасн
доведення електронних документів до виконавців, контроль стану виконання, зня
електронних документів з контролю, направлення виконаного електронн
документа до справи, облік, узагальнення й аналіз результатів виконання електрон
документів, інформування директора про хід та підсумки виконання електрон
документів.

До персональних даних в системі ІСУО мають доступ директор, вихова
методист, з обмеженнями – вихователі та вузькі спеціалісти.

Куратором створюються резервні копії найцінніших файлів для відновле
інформації при втраті оригіналу, з якого було створено резервну копію.

Інформація, яка обробляється в «КУРС: Дошкілля», підпадає під захист Зак
України «Про захист персональних даних».

IV РОЗДІЛ. Сайт закладу освіти

Сайт закладу освіти є невід`ємною частиною віртуального освітн
середовища закладу освіти, освітньої системи територіальної громади.

Сайт створюється з метою спрощення комунікації всіх учасників освітн
процесу; інформування громадськості про особливості закладу освіти, історії й
розвитку, про освітні програми та проєкти тощо; для позитивної презент
інформації про досягнення учнів (вихованців) та педагогічного колекти
дотримання принципу прозорості в діяльності закладу освіти та системати
інформування учасників освітнього процесу про діяльність закладу осв
впорядкування робочих процесів, активного впровадження інформаційн
комунікаційних технологій у практику роботи закладу освіти створення у
мережевої взаємодії закладу освіти з іншими установами.

Сайт закладу освіти функціонує відповідно до Положення про сайт зак
освіти. Функціонування сайту поєднує в собі процес збору, обробки, оформле

публікації інформації з процесом інтерактивної комунікації і в той же час презентує актуальний результат діяльності школи.

Сайт розміщено на українському сервері - http://219.dnz.zp.ua.

Сайт закладу освіти не розміщується на серверах в країнах або належних компаніям та громадянам країн (у тому числі й афілійованих з ними), з якими в України є невирішені політичні, торговельно-економічні чи військові конфлікти.

Дизайн сайту формується в рамках наявних можливостей і повинен відповідати цілям, завданням, структури та змісту офіційного сайту та критеріям технологічності, функціональності та оригінальності.

Перехід з одного розділу в інший розділ повинен бути доступний з будь-якої сторінки сайту.

Сайт повинен переглядатися за допомогою web-браузерів, що працюють в поширених операційних системах, у тому числі і для мобільних пристроїв (планшетні комп'ютери та смартфони). Загальний дизайн і функції сайту повинні зберігатися при перегляді в різних браузерах і при різній роздільній здатності екрану монітора.

Керівник закладу освіти призначає адміністратора/редактора сайту, який несе відповідальність за вирішення питань про розміщення інформації, про видалення чи оновлення застарілої інформації.

Адміністратор/редактор сайту має доступ до редагування матеріалів сайту в мережі Інтернет і несе персональну відповідальність за вчинення дій з використанням паролів для управління сайтом.

Сайт може бути закритий (перенесений на іншу адресу) тільки на підставі наказу керівника закладу освіти.

Адміністрація закладу освіти (керівник закладу та його заступник, відповідальний за інформаційне забезпечення освітнього процесу), адміністратор/редактор сайту, автори публікацій несуть персональну відповідальність за зміст інформації, розміщену на інформаційних ресурсах закладу.

Інформаційне наповнення сайту формується відповідно до вимог чинного законодавства, зокрема, відповідно до ст. 30 Закону України «Про освіту», та статутної діяльності закладу з суспільно-значущої інформації як для всіх учасників освітнього процесу, так і для інших зацікавлених осіб.

Інформаційні матеріали сайту закладу освіти подаються державною мовою та (за потреби) іншими мовами відповідно до вимог чинного законодавства України.

Відповідно до Закону України «Про засади запобігання та протидії дискримінації в Україні» на сайті закладу освіти повинні бути відсутні вияви дискримінації, щодо віку, раси, кольору, статі, мови, релігії, політичних або інших переконань учасників освітнього процесу, національного, етнічного або соціального походження, майна, інвалідності, народження або іншого статусу.

Сайт закладу освіти не має містити загрози для збільшення вразливості здобувачів освіти – не допускається розміщення на сайті інформації, забороненої для поширення серед неповнолітніх, а саме:

- інформаційні матеріали, які вміщують заклики до насильства, розпалювання соціальної та расової ворожнечі, міжнаціональних та релігійних чвар; екстремістські релігійні та політичні ідеї;
- інші інформаційні матеріали, які заборонені законодавством України.

Частина інформаційного ресурсу, який формується за ініціативи підрозділів, творчих колективів, педагогів, учнів, може бути розміщена на окремих блогах та сайтах, спеціалізованих сайтах, доступ до яких організовується із сайту закладу.

Забороняється розміщення на сайті закладу освіти інформації рекламн комерційного характеру та інформації, яка не належить до сфери діяльності установ

Сайт закладу освіти може містити ресурси обмеженого доступу (для певн категорій користувачів сайту).

Відповідальність за зміст інформації, що висвітлюється на сайті закладу освіт несе керівник закладу освіти та особи, відповідальні за інформаційну та програмн технічну підтримку сайту закладу освіти.

Для захисту сайту закладу освіти потрібно передбачити та забезпечити:

Технічний захист - це аспект безпеки, що стосуються захисту технічни ресурсів та інформаційних технологій від зловживання: захист від кібератак, вірусів шпигунського ПЗ, шахрайства та інших загроз. Технічна безпека може бути забезпечена шляхом автентифікації користувачів, надання права доступу обов'язкового резервного копіювання розміщених матеріалів, антивірусного програмне забезпечення.

Юридичний захист - це аспект безпеки, що стосуються дотриманн законодавства в галузі захисту персональних даних, прав на інтелектуальну власність авторського права, конфіденційності та інших правових питань. Для забезпечення юридичної безпеки, сайт має відповідати вимогам законодавства та політики захисту даних.

При розміщенні інформації на сайті необхідно забезпечувати дотримання вимог законодавства України про захист персональних даних. Всі матеріали про учасників освітнього процесу (керівників, викладачів, працівників, випускників, учнів допускаються до розміщення тільки з їх письмової згоди.

Заклад освіти забезпечує механізм, щоб здобувачі освіти та/або їхні батьки, або особи, які їх замінюють, мали безстрокове право скасувати свою згоду на обробку особистих даних, вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання яке здійснюється з порушенням вимог закону або коли це компрометує їхню гідність безпеку та конфіденційність.

Для дотримання політики академічної доброчесності забороняється розміщення на сайті закладу освіти контенту з порушенням авторських прав та умов ліцензування, контрафактних аудіо-, фото- та відеоматеріалів, примірників програмного забезпечення та посилання на такі матеріали.

Інформація про права людини та права дитини в цифровому середовищі розміщується на сайті закладу освіти для всіх учасників освітнього процесу.

Соціальний захист – це аспект безпеки, що стосуються відносин між людьми, які взаємодіють у цифровому освітньому середовищі: запобігання кібербулінгу, кіберзлочинності, дискримінації та інших соціальних проблем.

Етичний захист – це аспект безпеки, що стосуються етичних питань, які можуть виникнути в контексті використання цифрового освітнього середовища: питання конфіденційності, приватності, моральних принципів тощо. Для забезпечення етичної безпеки сайт закладу має чіткі правила та процедури, які визначають прийнятну поведінку в цифровому середовищі, а також враховувати вимоги до етичної поведінки в процесі розробки та використання цифрових технологій.

Сайт закладу освіти є офіційним портфоліо закладу освіти.

Контент закладу освіти оновлюється відповідно до потреби та відповідно до термінів, визначених законодавством України в галузі освіти.

З метою забезпечення права осіб, які є учасниками освітнього процесу, на приватність, визначаються загальні підходи до публікації фотографій чи відеозаписів, відеоматеріалів або творчих робіт дітей у мережі Інтернет.

Згідно із Законом України «Про захист персональних даних» при зарахуванні дитини до закладу освіти закладом освіти отримується обов'язково задокументована згода суб'єктів персональних даних. Оскільки суб'єктами персональних даних є неповнолітні особи, то згідно з нормами Сімейного та Цивільного кодексів України, згоду на обробку персональних даних дитини мають надати батьки або особи, які їх замінюють. Також батьки повинні подати згоду на обробку власних персональних даних. Із настанням повноліття особа надає таку згоду самостійно, і батьки вже не мають права визначати межі обігу персональних даних їхніх дітей.

З урахуванням обмежень, визначених Цивільним кодексом України (ЦКУ), ст. 307, 308, допускається здійснення відео-та фотозйомки навчальних занять, розміщення цих матеріалах на офіційних ресурсах закладу освіти без зазначення персональних даних учнів, педагогів, локації (на період дії воєнного стану).

Крім того, якщо щодо дитини або педагога вчиняються протиправні дії і зйомка ведеться з метою їх фіксації, така зйомка може визнаватися допустимою, враховуючи положення частини другої статті 32 Конституції України, відповідно до яких збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди можливі, зокрема в інтересах прав людини.

Заклад освіти зобов'язується повідомляти батьків, або осіб, що їх замінюють, про публікацію фото-, відеоматеріалів за участю їхніх дітей.

З метою дотримання авторського права матеріали (наприклад, відеозапис або презентація уроку, пам'ятки, рекомендації тощо), розроблені працівником закладу освіти, розміщується на сайті закладу освіти з інформацією про автора.

В разі використання на сайті закладу освіти матеріалів, розроблених іншими особами та розміщених у вільному доступі в інтернеті, поряд з розміщеними матеріалами обов'язково зазначається авторство та/або подається покликання на використане джерело.

V РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (електронна пошта закладу освіти)

Електронна пошта – це послуга Інтернету, призначена для пересилання комп'ютерними мережами повідомлень (електронних листів) від користувача одному чи групі адресатів.

Електронна пошта для закладу освіти є одним із способів комунікації між всіма учасниками освітнього процесу, дозволяє швидко та зручно обмінюватись листами, інформацією, повідомленнями, матеріалами для навчання.

Не використовуються поштові сервіси, електронні поштові скриньки, заборонені на території України (згідно з Указом Президента від 15.05.2017 №133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»).

Для формування адреси електронної скриньки під час реєстрації обирається унікальне ім'я, яке буде використовуватися в електронній адресі, встановлюється пароль для облікового запису.

Визначено електронну пошту (ел.пошта) закладу освіти: _dnz219zpe@gmail.com

Визначається відповідальна особа за зміну паролів та налаштування додатк параметрів облікового запису. Змінений пароль повідомляється керівнику зак освіти.

Закладом освіти визначається режим використання особистих акау встановлюються правила використання поштових скриньок для співробітників.

Особиста ел.пошта використовується працівниками закладу освіти особистого листування.

Доступ та захист інформації є важливими аспектами роботи з електрон поштою в закладі освіти.

Управління доступом передбачає:

1. Створення ідентифікаційних облікових записів для кожного працівника, щ забезпечити індивідуальний доступ до електронної пошти.

2. Запровадження рівневого доступу на основі потреб та ролей працівни Наприклад, хто має право на адміністрування системи, хто може мати доступ конфіденційної інформації тощо.

3. Антивірусний захист: встановлення надійного антивірусного програмн забезпечення на комп'ютери та сервери, щоб захистити від вірусів, шкідлив програм та інших загроз безпеці. Періодичне оновлення антивірусних баз даних.

4. Створення паролів:

- запровадження політики паролів закладу освіти, яка встановлює вимоги що довжини, складності та унікальності паролів.

- забезпечення навчання працівників щодо безпеки електронної пош включаючи розпізнавання фішингових атак, зловмисних вкладень та інших загроз.

5. Оновлення паролю та регулярна архівація є важливими процедурами д забезпечення безпеки електронної пошти в освітній установі.

Зобов'язання користувачів корпоративної електронної пошти закладу осві визначається закладом освіти.

Працівники закладу освіти зобов'язані використовувати корпоратив електронну пошту при здійсненні своїх посадових обов'язків, зокрема, відправляти отримувати електронне листування внутрішнім і зовнішнім кореспондентам використанням адреси робочої пошти.

Працівник закладу освіти не має права:

а) використовувати електронну пошту закладу для цілей, не пов'язаних виконанням посадових обов'язків в закладі освіти;

б) повідомляти пароль доступу до адреси скриньки іншим особам;

в) здійснювати масову розсилку листів зовнішнім адресатам, в тому числі лист рекламного характеру;

г) розсилати листи, що містять:

- конфіденційну інформацію, доступ до якої обмежено чинним законодавство у тому числі містить державну таємницю, матеріали, використання яких порущ права власності;

- недостовірну інформацію, а також інформацію, що ображає честь і гідніст осіб, ганьбить ділову репутацію, пропагує ненависть або дискримінацію людей р расовими, етнічними, статевими, релігійними, соціальними ознаками, закликає д протиправних дій;

- матеріали, що містять віруси або інші комп'ютерні коди; файли, програм призначені для порушення, знищення або обмеження функціональності будь-яко комп'ютерного обладнання.

Відповідальність за зберігання паролів для корпоративних облікових записів покладається на адміністратора, а в разі зміни пароля користувачем – на користувача.

Обов'язок дотримуватись правил користування корпоративною електронною поштою, акантом, наданим закладом освіти, вноситься до посадових обов'язків працівника.

VI РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (соціальні мережі, месенджери)

Однією із критично значущих складових управлінського процесу у закладі освіти є інформування учасників освітнього процесу та громади про свою діяльність на відкритих загальнодоступних ресурсах.

Інформаційна відкритість забезпечується наявністю у закладі освіти майданчиків для інформування учасників освітнього процесу, у тому числі у соціальних мережах, месенджерах.

Сторінки освітніх закладів у соціальних мережах мають свої особливості, які зумовлені властивостями електронної комунікації: оперативність розповсюдження інформації; доступність; спрощений пошук цільової аудиторії; легкість налаштування зворотного зв'язку тощо.

В закладі освіти мережева комунікація здійснюється в Facebook, *Twitter*, *YouTube:* *https://www.facebook.com/dnz219*, *https://www.youtube.com/channel/UCNMiIHAecJx64skE3U7qNbQ*

Керівник закладу освіти спільно з педагогічним колективом визначають зміст (про що) і формат (як) буде здійснюватись інформування громадськості про діяльність закладу освіти, обговорюють обмеження щодо висвітлення інформації певного змісту.

Керівник закладу освіти призначає адміністратора або адміністраторів (за наявності кількості мереж), які несуть відповідальність за оприлюднення достовірної, точної та повної інформації, а також у разі потреби перевіряють правильність та об'єктивність наданої інформації і оновлюють оприлюднену інформацію.

Адміністратор сторінки закладу освіти у соціальній мережі дає дозвіл/запрошує приєднатися до шкільної спільноти користувачів соцмереж. Окрім того відповідальна особа (адміністратор сторінки) проводить щоденний моніторинг сторінки у соціальних мережах на предмет розміщення на них несанкціонованої інформації; підвищення онлайн культури спілкування учасників освітнього процесу; збереження персональних даних учасників освітнього процесу.

До несанкціонованої інформації можуть відноситися інформаційні матеріали, які вміщують заклики до насильства, розпалювання соціальної та расової ворожнечі, міжнаціональних та релігійних чвар; екстремістські релігійні та політичні ідеї; інформація, заборонена для поширення серед неповнолітніх; інформації рекламно-комерційного характеру та інформації, яка не належить до сфери діяльності освітнього закладу; інші інформаційні матеріали, які заборонені законодавством України.

Мову інформації на сторінці закладу освіти в соціальній мережі визначають закони України «Про освіту», «Про забезпечення функціонування української мови як державної», інші закони України та міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

З метою недопущення отримання зацікавленими особа
додаткової (приватної) інформації стосовно особи, членів її сім'ї, колег на сторі
освітнього закладу в соціальних мережах не публікується інформація, що мо
поставити під загрозу особисте життя особи, життя членів її сім'ї та інших о
обмежується доступ до приватної інформації в налаштуваннях конфіденційно
соціальної мережі; здійснюються налаштування, які найбільше захищають додатк
відомості про власника аканта, зокрема, не зазначається геолокація (мі
розташування освітнього закладу); здійснюється періодичний перегляд спи
«друзів» у соціальній мережі (*якщо серед них є незнайомі або підозрілі акаун
необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого об
приватної інформації про особу*); не використовуються соціальні мережі та пошук
системи (у т.ч. із застосуванням сервісів VPN), доступ до яких обмежено відпові
до Указу Президента України «Про застосування, скасування і внесення змін
персональних спеціальних економічних та інших обмежувальних заходів (санкцій)

Керівник закладу освіти відповідає за визначення завдань, забезпечення
контроль за діяльністю відповідальної особи з питань опрацювання, оприлюдне
публічної інформації, передбаченої чинним законодавством.

Для будь-яких контактів чи комунікації між учасниками освітнього про
закладу освіти використовуються спільноти в месенджері.

В закладі освіти таким засобом комунікації виступають *Telegram-спільно
Viber-спільноти, Padlet-дошки.*

Спільноти, сформовані для комунікації та різного роду інформування учасн
освітнього процесу, класифікуються за призначенням: для інформування учасн
освітнього процесу про новини закладу освіти; для спілкування педагогіч
працівників з адміністрацією; для спілкування вчителів та учнів класу чи парал
для обміну інформацією між вчителем та батьками класу та інші.

Створюються відкриті спільноти – приєднатись може будь-хто; закрит
призначені для обмеженої кількості учасників, яких запрошує адміністратор.

Керівник закладу освіти призначає відповідального адміністратора чи декіл
осіб для ведення загальношкільної спільноти.

Для всіх інших спільнот за потребою адміністратором може виступати той,
створює спільноту.

Адміністратор спільноти визначає її правила, в тому числі дозволяє
забороняє учасникам відправляти повідомлення у спільноту.

Спілкування може бути одностороннім (повідомлення пише лише адміністра
а учасники можуть лише читати, ставити позначки та пересилати їх)
двостороннім (учасники спільноти також можуть надсилати повідомлення).

Адміністратор може змінювати правила спільноти відповідно до ситуації.

В закладі освіти обговорюються та приймаються загальні підходи в
використання месенджерів для функціонування спільнот, зокрема, визначаю
обмеження щодо розміщення в спільноті певного контенту.

Інформація, розміщена в спільноті, доступна для всіх його учасників незале
від того, коли вони приєдналися. Вся історія спілкування зберігається в чаті.

В закладі освіти встановлюються чіткі правила – як для працівників, так і
учнів – щодо спілкування в чатах.

Загальні правила щодо спілкування в чатах обговорюються на засіда
колегіального органу управління закладом освіти (педради), органів самоврядува

(зокрема, учнівського, батьківського), додаються до правил поведінки (внутрішнього розпорядку), прийнятих в закладі освіти.

Правила спілкування в чатах (можуть бути додатком до Положення, розділом Правил поведінки або окремим документом)

– *Поважайте чужі часові рамки, бережіть особистий час. Встановіть та дотримуйтесь часових обмежень для надсилання повідомлень (наприклад, не писати у чат після 20:00).*

– *Дотримуйтесь контексту та тематики групи. Не засмічуйте групові чати зайвою, неактуальною інформацією. Пам'ятайте про мету спілкування, чітко розумійте, для чого ви щось говорите, наскільки конструктивним і доречним це буде.*

– *Не поширюйте неперевірену інформацію.*

– *Турбуйтесь про співрозмовників – передавайте інформацію повно, але, водночас, лаконічно.*

– *Перевіряйте корисність повідомлення: під час відправлення на цілу групу воно повинно стосуватися кожного члена чату. Інакше варто скористатись чатом 1-1. Уважно ставтеся до повідомлень у спільному чаті: іноді ми поспішаємо із відповіддю і перепитуємо про те, що в чаті вже написали.*

– *Не ображайте учасників чату, дотримуйтесь етики спілкування, принципів толерантності, відкритості, свободи думки, совісті і переконань,*

– *Дотримуйтесь правил мережевого етикету: використовуйте зрозумілу мову, транслюйте правильний тон і настрій, пишіть грамотно (помилки у словах тощо – значно знижують якість розмови та ускладнюють взаєморозуміння), не переобтяжуйте повідомлення текстом, стікерами й емодзі, уникайте потенційно образливих слів та висловів, а також того, що у письмовій формі може бути трактовано двозначно, неправильно.*

– *Не використовуйте нецензурну лексику, саморекламу, спам.*

– *Уникайте переходу на особистості та оціночних суджень, не допускайте будь-яких форм дискримінації.*

– *Дотримуйтесь правила емоційної рівноваги. Не пишіть в чат під час емоційного навантаження, стресу. Основа екологічного спілкування – це доброзичливий тон та взаємна підтримка.*

– *За порушення правил вводиться обмеження: адміністратор може тимчасово видаляти учасника або відправляти у бан на певний час.*

– *Будьте чесними та уважними – лише тоді спілкування залишатиметься щирим та довірливим.*

Правила закріплюються у чаті за допомогою відповідної функції закріплення повідомлень.

Презентація закладу освіти в соцмережах, здійснення спілкування його працівників в месенджерах має бути коректним, професійним, етичним. Важливо сформувати у працівників закладу освіти розуміння ризиків втрати онлайн-репутації – власної та закладу освіти.

Між приватним та професійним життям учителів, зокрема, й у цифровому середовищі, важливо встановити чітку межу.

Для будь-яких контактів між співробітниками закладу освіти та учнями/вихованцями та/або батьками в закладі освіти використовується корпоративна (офіційна) електронна пошта.

Для безпеки педагогів варто створити окремий обліковий запис або окремо користувача, якщо пристроєм – комп'ютером, ноутбуком, планшетом – вдома чи роботі користується кільки користувачів, розмежувати власні електронні скрин для особистого користування та для робочих питань.

Комунікаційна політика закладу освіти забороняє (*обмежує*) будь-які контак не пов'язані з освітньою діяльністю, та контакти на платформах, що не мають стосунку до закладу. *В разі обмежень – прописати їх.*

На випадок проведення відеоконференцій або занять у віддаленому режи закладом освіти установлюються чіткі приписи як для співробітників, так і д здобувачів освіти (наприклад, що бажано підготувати місце для віддалено заняття/сеансу зв'язку та подбати про тих, хто перебуває поруч – чи то вдома, чи т класі).

VII РОЗДІЛ. Особливості організації освітнього процесу.

Організація освітнього процесу в закладі відбувається відповідно нормативних документів Міністерства освіти і науки України, згідно зі статут закладу освіти, з урахуванням стану функціонування освітнього середовища закла освіти, його матеріально-технічних, системотехнічних, кадрових можливосте стратегічних перспектив розвитку закладу освіти.

Забезпечення цифрової безпеки необхідно в умовах організації освітньо процесу за дистанційною формою та/або з використанням технологій дистанційно навчання.

Для забезпечення діяльності закладу освіти в умовах режиму дистанційно навчання в закладі освіти прийнято Стратегію (*Положення*) дистанційного навчанн яким узгоджено правила та алгоритми взаємодій усіх учасників освітнього проце для виконання освітніх програм закладу в даному форматі надання освітніх послуг.

Для організації дистанційного формату навчання в закладі освіти визначен онлайн-платформу – Google-таблиця, розміщену на платформі Google та онлай ресурс Padlet-дошка.

На обраній платформі створено акаунти всіх учасників освітнього процесу дл забезпечення захисту даних та надання визначеного для певної категорії учасник освітнього процесу рівня доступу до матеріалів платформи.

Визначено перелік сервісів для проведення відеоконференцій та онлай зустрічей (*ZOOM, GoogleMeet, Teams*) в закладі освіти для здобувачів освіти різни вікових категорій.

З метою захисту персональних даних під час дистанційного навчанн забезпечується дотримання вимог щодо захисту персональних даних учасників

Організовано ознайомлення учасників освітнього процесу з політикою заклад освіти, що регулює використання інформаційних технологій (сервісів, ресурсів різними учасниками освітнього процесу. На початку навчального року проводитьс обов'язкове ознайомлення педагогів з переліком ресурсів, які використовуватимуться в навчанні, надаються інструкції до роботи з вказаними з цифровими інструментами.

Закладом освіти проводяться заходи щодо дотримання авторського права.

Відповідно до Положення про академічну доброчесність (затвердженого наказом від 31.12.2021 № 128/р) в закладі освіти забезпечується дотримання академічної доброчесності всіма учасниками освітнього процесу.

VIII РОЗДІЛ. Проведення заходів просвітницького характеру

З метою дотримання права дитини на безпеку та захист, яке є базовим та поширюється на її життєдіяльність як онлайн, так і офлайн, з урахуванням пріоритетного значення цифрових компетентностей для ефективного навчання та успішного життя людини в сучасному світі, формування навичок безпечної поведінки дитини в цифровому середовищі з раннього віку в закладі освіти проводиться система профілактичних заходів просвітницького характеру з підвищення рівня знань в області інформаційно-комунікативних технологій, з питань безпечної поведінки в інтернеті, медіаграмотності.

Для організації роботи з учасниками освітнього процесу в закладі освіти здійснюються наступні кроки:

1. Визначаємо складові формування навичок безпечної поведінки в цифровому середовищі, зокрема, права людей (зокрема, права в цифровому середовищі); електронна участь (в ухваленні рішень); збереження здоров'я під час роботи з цифровими пристроями; механізми захисту прав, що порушуються в інтернеті, а також способи отримати допомогу.

2. Визначаємо коло осіб, які причетні до цифрової комунікації учасників освітнього процесу: педагоги, здобувачі освіти (вихованці), батьки, інші особи, з якими може бути налагоджено (можуть бути учасниками) організацію таких заходів.

За відповідними напрямками складається Програма просвітницької роботи (або план проведення просвітницьких заходів на навчальний рік) для всіх категорій учасників освітнього процесу.

Програма просвітницької роботи може містити інформацію про загальні напрямки роботи. План проведення просвітницьких заходів на навчальний рік містить конкретні заходи, терміни проведення, інформацію про залучених осіб тощо.

Програма просвітницької роботи може бути реалізована впродовж навчального року або за певний визначений період (наприклад, під час Тижня цифрової грамотності відповідно до річного плану роботи закладу освіти)

До Програми просвітницької роботи можуть вноситись зміни з урахуванням динамічного розвитку цифрових технологій та відповідно до актуальних потреб учасників освітнього процесу.

Орієнтовна Програма просвітницької роботи з учасниками освітнього процесу.

І Просвітницькі заходи з педагогами (вихователями) як суб'єктами гарантування цифрової безпеки.

Просвітницькі заходи з працівниками закладу освіти спрямовуються на підвищення рівня цифрової компетентності.

Попередньо визначається рівень спроможності педагогів працювати у цифровому середовищі з урахуванням того, що *педагогам необхідно:*

- володіти інформацією щодо можливостей цифрових технологій;
- формувати вміння вибрати ту технологію, цифрові інструменти, які відповідають його педагогічній діяльності;
- бути тренером (ведучим) у процесі формування навичок комунікації дітей, батьків з питань поведінки у цифровому просторі;
- вміти оцінювати отриману інформацію з точки зору реалізації в професійній діяльності та визначати особисті потреби у підвищенні кваліфікації в даній сфері;

- вміти виступати посередником під час соціальної активності між всіма учасниками освітнього процесу.

Для забезпечення правильного формування цифрової компетентності педагога він повинен мати:

- навички володіння методами та прийомами інформаційної діяльності;
- сформовані професійні навички та уміння, що забезпечуються використанням цифрових технологій у роботі;
- можливість безпосереднього використання знань, умінь і навичок використання цифрових технологій у професійній сфері;
- мотивацію до удосконалення знань та вмінь використання цифрових технологій в професійній діяльності та житті;
- можливість забезпечення розвитку професійних якостей працівника, підвищення рівня освітніх послуг за допомогою цифрових технологій.

№ з/п	Просвітницькі заходи	Примітки
1.	Для підвищення рівня обізнаності освітян щодо небезпек в мережі Інтернет: організація семінарів та навчальних курсів для освітян з питань цифрової безпеки, які охоплюють теми захисту персональних даних, безпеки паролів, використання безпечних мереж Wi-Fi, виявлення фішингових атак та інші аспекти цифрової безпеки.	Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
2.	Для здобуття освітянами цифрової освіти з використанням інформаційних ресурсів: підготовка та розповсюдження матеріалів: пам'яток, брошур або інші матеріали з цифровою безпекою, які освітяни можуть використовувати в своїй роботі з учнями та вихованцями; надання вихователям як суб'єктам гарантування цифрової безпеки доступу до актуальних інформаційних ресурсів та рекомендацій з цифрової безпеки.	Згідно з ключовими положеннями, передбаченими Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
3.	Для обміну досвідом освітян як суб'єктів гарантування цифрової безпеки: створення форуму або онлайн-спільноти, де працівники закладу освіти зможуть обмінюватися досвідом та кращими практиками з цифрової безпеки; ділитися успішними стратегіями використання цифрових інструментів в професійній діяльності.	

	Для підвищення рівня медіакультури та медіаграмотності: проведення тренінгів та майстер-класів для освітян з використанням сучасних інструментів для створення пізнавальних ігор та інтерактивних ресурсів; створення/перегляд/обговорення методики використання спеціальних мультиплікаційних відеороликів, які наголошують на безпеці в Інтернеті для дошкільнят; встановлення партнерства з місцевими медійними організаціями або журналістами для проведення майстер-класів, тренінгів або стажування для учнів, де вони зможуть поглибити свої знання з медіа грамотності.	Згідно з реалізацією напрямів Стратегії інформаційної безпеки на період до 2025 року, затверджена указом Президента України від 28.12.2021 №685/2021
5	Для підвищення рівня інфомедійної культури педагогів в соціальних мережах: сприяння участі педагогів у вебінарах, прослуховуванні навчальних курсів, тренінгах, інтерактивних формах навчання, які формують складові інфомедійної культури дорослого особисто та як тренера для дітей у подальшому.	
6	Для підвищення практичних вмінь педагогів щодо побудови партнерських взаємовідносин між закладом освіти і родиною з питань безпечної поведінки дитини у цифровому середовищі: проведення тренінгів для формування навичок комунікації з батьками з питань поведінки у цифровому просторі; формування навичок стимулювання у батьків соціальної активності щодо обміну досвідом з питань формування безпечної поведінки дітей у цифровому просторі.	МОНУ (№1/9-128 від 10.03.2021 «Щодо необхідності проведення додаткових профілактичних заходів в середовищі дітей та підвищення обізнаності батьків»).

Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки з вихованцями:

Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки можуть включати формування цифрових компетентностей для навчання та життя, ознайомлення з основами кібербезпеки, правилами безпечної роботи в Інтернеті, інформування про коректне використання антивірусного програмного забезпечення та інших інструментів захисту від кібератак.

1. Визначення рівня умінь дітей дотримуватись правил безпечної поведінки в інтернеті:

- не розповсюджує особисті дані (адресу проживання, місце навчання, номер мобільного телефону, інформацію про батьків) в Інтернеті;

- якщо трапилась неприємна ситуація – звертається по допомогу до дорослих, кому дитина довіряє (батьки, старший брат чи старша сестра, вихователь у садочку);

- не зустрічається (не прагне зустрітись) з тими, кого ми знаємо тільки онлайн;

- не відповідає на повідомлення, які є неприємними, повідомляє про них дорослому;

- розповідає (готовий розповісти) батькам, якщо хтось надсилає чи говорить неприємні слова;

- ні з ким не ділиться (знає правило) своїм паролем до гаджету чи додатку, доступом до власного профілю в соцмережі тощо;

- перед завантаженням нового додатку запитує (запитає) дозволу у батьків (діти 4-6(7) років).

2. Відповідно до отриманих результатів щодо рівня умінь дітей дотримуватись правил безпечної поведінки в цифровому просторі визначаються напрямки/відповідні заходи просвітницького характеру з учнями (вихованцями).

3. До заходів просвітницького характеру з учасниками освітнього процесу (вихованці) щодо попередження інформаційної небезпеки включаються заходи щодо медіа грамотності, формування культури кібербезпеки та інфомедійної культури у цілому.

№ з/п	Просвітницькі заходи	Примітки
1.	Для навчання правилам безпечної поведінки вихованців в Інтернеті: організація розважальних активностей, які сприяють розвитку безпечної поведінки в Інтернеті для дітей старшого дошкільного віку; використання спеціально розроблених інтерактивних ігор, які закріплюють правила безпечної поведінки в онлайн-середовищі; створення та проведення інтерактивних ігор та квіз-конкурсів на тему кібербезпеки, де діти зможуть вирішувати завдання, пов'язані з безпекою в Інтернеті.	Вікова категорія до 7 років Згідно з реалізацією напрямів Стратегії інформаційної безпеки на період до 2025 року, затверджена указом Президента України від 28.12.2021 №685/2021 Згідно з напрямами Стратегії кібербезпеки України, затвердженої указом Президента України від 26.08.2021 №447/2021

Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки з батьками (іншими дорослими, які опікуються вихованням дитини):

1. Проведення заходів щодо визначення ступеню розуміння батьками питання безпеки комунікації дитини у цифровому просторі.
2. Актуалізація визначення рівня довіреності відносин дітей та батьків.

3. Опитування батьків щодо засобів комунікації, якими користується дитина у цифровому просторі.

4. Плануванні заходів для батьків щодо попередження інформаційної небезпеки з урахуванням актуальних потреб учасників освітнього процесу.

Просвітницькі заходи	Зміст заходів
1.	Батьки у цифровому суспільстві
1.1. Цифрове суспільство	Використання цифрових технологій та сервісів для: – розуміння ролі цифрових ресурсів у житті громадянина та суспільства; – вирішення проблем та завдань у повсякденному житті, особистої взаємодії, спілкування, перегляду ресурсів, даних та відомостей; – участі у суспільній діяльності; – захисту своїх прав та свобод, вираження власної громадянської позиції
1.2.Електронне урядування	Використання цифрових технологій та сервісів для: – підтримки та участі у електронному урядуванні; – розуміння понять «відкриті дані», «електронна ідентифікація громадян», «цифрові державні платформи» тощо;
1.3. Електронний заклад освіти	Використання цифрових сервісів та технологій для: – створення «цифрового робочого місця» дитини; – розуміння цифрового освітнього середовища закладу (групи); – заохочення батьків та громадськості до ефективного використання цифрового освітнього середовища закладу (групи); – активного сприяння використанню цифрових технологій для комунікації із закладом освіти.

Безпека в цифровому суспільстві	Використання цифрових сервісів та технологій для: – розпізнавання та протидії маніпуляційних технологій пропаганди, перевірки надійності джерел і достовірності даних небезпек в цифровому просторі; – розуміння важливості відповідальної і безпечної поведінки цифровому просторі; – уникнення ризику здоров'я і загроз для фізичного психологічного благополуччя при роботі у цифровому просторі; – запобігання онлайн-злочинів в цифровому суспільстві; – формування вміння захистити цифрові пристрої, дані та інш ресурси; – знання заходів безпеки, розуміння персонально відповідальності кожного щодо ризиків та загроз пр використанні цифрових пристроїв і мереж; – захисту персональних даних та приватності; –захисту навколишнього середовища, тобто розуміння впливу цифрових технологій на навколишнє середовище, з точки зору їх утилізації, а також їх використання, що може нанести шкоду наприклад, об'єктам критичної інфраструктури тощо
2. Розвиток цифрової компетентності батьків Використання цифрових сервісів для спілкування, співпраці батьків та закладу освіти	
2.1. Комунікація. Використання цифрових сервісів для покращення комунікації батьків із закладом освіти або третіми особами. Розвиток співпраці та вдосконалення організаційних стратегій комунікації	Використання цифрових сервісів для: – участь у онлайн-заходах для спілкування з закладом освіти, дотримання, наприклад, правил, зустрічі, заходів тощо; – отримання інформації (індивідуально або колективно) від закладу освіти, наприклад, про особистий прогрес дитини у навчанні та з проблемних питань, що викликають стурбованість; – спілкування з іншими батьками (різними педагогами) в в закладі освіти; спілкування з третіми особами, які мають відношення до освітнього процесу; – вміння отримувати інформацію за допомогою вебсайту закладу освіти або через соціальні мережі, освітні платформи, інші цифрові сервіси; – участь у співпраці учасників освітнього процесу.

2.2. Інформаційна компетентність та медіаграмотність	Використання цифрових сервісів як уміння: - формулювати власні інформаційні потреби, здійснювати пошук цифрових даних та цифрових ресурсів в цифровому освітньому середовищі та в Інтернеті; - аналізувати, порівнювати і критично оцінювати надійність цифрових джерел і достовірність даних, інформації та цифрових ресурсів; - розміщувати, зберігати та видаляти цифрові дані та ресурси у цифровому середовищі; - структурувати цифрові дані та інформацію в цифровому середовищі.
2.3. Відповідальне використання цифрових технологій та сервісів	Для використання цифрових сервісів - усвідомлення впливу цифрових технологій на навколишнє середовище та соціум; - розуміння ризиків і загроз цифрового суспільства; -розуміння заходів власної безпеки у цифрових середовищах; - уникнення ризиків для здоров'я і загроз для фізичного і психологічного благополуччя; - захист особистих даних і конфіденційності у цифрових середовищах; - захисту себе і інших від можливих небезпек у цифрових середовищах.
2.4. Вирішення проблем за допомогою цифрових технологій та сервісів	Під час використання цифрових сервісів: - виявлення технічних проблем у роботі пристроїв і використанні цифрових середовищ і їх вирішення; - регулювання і налаштування цифрових середовищ для власних потреб; — визначення, оцінювання, добору і використання цифрових сервісів і можливі технологічні реакції з метою подальшого вирішення цих завдань або проблем; - виявлення прогалин у власній цифрової компетентності щодо налаштування цифрових пристроїв і сервісів; - підтримки інших в розвитку їх цифрової компетентності щодо налаштування цифрових пристроїв і сервісів; - пошуку можливостей для саморозвитку в галузі цифровізації.
3. Використання та аналіз цифрових ресурсів	