додаток 1
до наказу ЗДО №290
від 02.01.2026 №07/р

ЗАТВЕРДЖЕНО
наказом директора
Закладу дошкільної освіти №290 «Зайчатка»
Запорізької міської ради
від «02» січня 2026 року № 07/р

ЗАКЛАД ДОШКІЛЬНОЇ ОСВІТИ №290 «ЗАЙЧАТКА»
ЗАПОРІЗЬКОЇ МІСЬКОЇ РАДИ
(ЗДО №290 ЗМР)

ПОЛОЖЕННЯ
Про цифрову безпеку закладу освіти заклад дошкільної освіти № 290 «Зайчатка» Запорізької міської ради (ЗДО №290 ЗМР)

м. Запоріжжя

2026

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 10

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. .....

V РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (ел. пошта закладу освіти) 14

VI РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (соціальні мережі, месенджери) 15

VII РОЗДІЛ. Особливості провадження освіти, дистанційної освіти 18

Організація освітнього процесу. Особливості дистанційної освіти .....

VIII РОЗДІЛ. Проведення заходів просвітницького характеру 19

IX РОЗДІЛ. Захист персональних даних в цифровому середовищі закладу освіти 26

X РОЗДІЛ. Прикінцеві положення 27

Використані джерела: 28

ПОЛОЖЕННЯ

Про цифрову безпеку закладу освіти

І РОЗДІЛ. Загальні положення

Положення «Про цифрову безпеку закладу освіти» визначає політику цифрової безпеки закладу освіти №290 «Зайчатка» ЗМР.

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

Положення розроблене з урахуванням вимог законів України «Про дошкільну освіту», законів України, дія яких поширюється на впровадження та використання інформаційних технологій у сфері освіти в Україні: «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні комунікації», «Про основні засади забезпечення кібербезпеки України», «Про електронні документи та електронний документообіг».

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

У Положення нижче наведені терміни вживаються в такому значенні:

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

безпека мережі - здатність електронних комунікаційних мереж протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж, а 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 електронними засобами;

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

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

електронні інформаційні ресурси - систематизовані відомості і дані, створені, оброблені та збережені в електронній формі за допомогою технічних засобів та/або 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;

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, визначених законодавчими актами України.

ІІ РОЗДІЛ. Системотехнічне забезпечення цифрового освітнього простору закладу освіти

Цифровий освітній простір закладу освіти складають наступні компоненти:

внутрішні: комп'ютери, засоби відеоспостереження, цифрове діловодство;

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

Забезпеченість робочими комп'ютерами

1. Загальна кількість персональних комп'ютерів та ноутбуків в закладі освіти складає 7 (з них в робочому стані -7, не працюють 0)

2. Із загальної кількості персональних комп'ютерів (в робочому стані) - 7:

- робочі місця з комп'ютером – 3- у кабінеті директора, робочі місця з ноутбуком - кабінет методиста,кабінет завгоспа, кабінет сестри медичної.

В користуванні адміністрації: 1- стаціонарний комп'ютер, 2 – портативних комп'ютерів.

3. В користуванні педагогічних працівників – 2– стаціонарних,2–портативних ,що складає 57% (відсотків від загальної кількості працюючих комп'ютерів).

4. В користуванні адміністрації – всього 1-стаціонарний комп'ютер, що складає 14%

(відсотків від загальної кількості працюючих комп'ютерів в ЗДО), 2 – портативних, що складає 28% (відсотків від загальної кількості працюючих комп'ютерів в ЗДО.

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

6. Кількість персональних комп'ютерів версії операційних систем – Windows (7,10,11) : Windows 10-1шт, Windows 7- 5шт, Windows-1.

Налаштування та обслуговування комп'ютерів працівників Ліцензійне

програмне забезпечення

Порядок оновлення доступу при звільненні працівника

Для забезпечення цифрової безпекив закладі освіти при звільненні працівника виконуються наступні дії:

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

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

3. Працівник, що звільняється, має передати матеріальні цінності (пристрої), надані йому в користування уповноваженій особі.

4. Уповноважена особа має оглянути пристрої, якими користувався працівник, що звільняється, впевнитись в їх справності/скласти акт про несправність та повідомити керівництво закладу.

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

6. Особа, відповідальна за створення корпоративних акаунтів, має видалити обліковий запис працівника, що звільняється, впродовж/не пізніше наступних 5 днів після звільнення працівника.

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

Збереження інформації

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

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

Встановлення, збереження та оновлення паролів на всіх інформаційних та технічних ресурсах освітнього закладу (адмінські паролі (сайт, база даних закладу, платформа для дистанційного навчання), ключі шифрування, паролі до роутера і т.п.).

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

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

Робота з паролями

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

Для збереження паролів використовується:

- паперовий варіант – зберігається в сейфі адміністрації закладу;

- менеджер паролів – спеціальна програма, яка надає можливість тримати паролі у безпеці завдяки шифруванню. Потрібно пам'ятати один пароль для доступу до іншої бази (Google Password Manager, тощо).
- текстовий документ – зберігається документ в архіві під паролем;
- резервне копіювання для кожного способу.

Доступ до інформації та місця збереження паролів має представник 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. Слідкувати за оновленнями: переконатися, що отримуються автоматичні оновлення від служби Windows Update і інсталювати всі необхідні для організації оновлення.
4. Заборонити інсталювати програмне забезпечення з-поза меж організації, яке не затверджено або не адмініструється у закладі.
5. Безпечно зберігати дані. Заклад надає ресурс для зберігання даних, як-от GoogleDrive або інше корпоративне сховище. Не зберігати дані лише на локальному комп'ютері.
6. Постійно нагадувати (створювати пам'ятки, викладати їх на видне місце) щодо правил безпеки.

II. Створити групи в хмарному середовищі.

GoogleDrive – пакет спеціалізованого хмарного програмного забезпечення й інструментів для спільної роботи від компанії Google.

III. Налаштувати наступні рівні захисту:

1) фізичний (на фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій);

2) програмно-технічний (на програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності) ;

3) управлінський (на рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки);

4) технологічний (на технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій);

5) рівень користувача (на рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища);

6) мережевий (на мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою);

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 (оптичний волокно).

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

На ПК встановлено тип підключення до мережі – 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	Linet
Тип підключення закладу освіти до мережі Інтернету (бездротовий Wi-Fi або провідний Ethernet)	провідний Ethernet
Налаштування доступу до мережі Інтернету закладу освіти шляхом введення облікових даних, таких як ім'я користувача та пароль	так
Встановлення рівня доступу до мережі на ПК	вільне

ІІІ РОЗДІЛ. Електронне діловодство закладу освіти

Ведення електронного діловодства в закладі освіти здійснюється відповідно до чинного законодавства та регламентується наказами Міністерства освіти і науки України від 08.08.2022 № 707 «Про затвердження Інструкції з ведення ділової документації у закладах загальної середньої освіти в електронній формі», від 25.06.2018 № 676 «Про затвердження Інструкції з діловодства у закладах загальної середньої освіти».

Термін зберігання документів регламентується Переліком типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів (наказ Міністерства юстиції України від 12.04.2012 № 578/5), Переліком відомчих (галузевих) документів.

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 одного з хмарних рішень для роботи з документами – Google Drive на корпоративній платформі Google, яка схвалена педагогічною радою та якою володіє та централізовано керує заклад освіти.

Найцінніші файли закладу зберігаються в хмарному сховищі, на спільних дисках в домені закладу – https://drive.google.com/drive/u/0/home

Доменне ім'я зареєстроване на заклад.

Власником файлів, які зберігаються в хмарному середовищі закладу освіти, є заклад освіти, а не окремий працівник, який їх створює або додає. Заклад освіти є власником всього контенту, що створюється та зберігається в межах платформи, у тому числі, після звільнення окремих працівників, які їх створювали або додавали.

Адміністратором корпоративної платформи (основний обліковий запис із максимальним доступом до платформи закладу освіти) є відповідальна особа, людина призначена наказом керівника закладу освіти.

Додатковим адміністратором, на випадок відсутності/недоступності основного адміністратора, має бути керівник (вихователь-методист) закладу освіти.

Адміністратор може заборонити користувачам поширювати певні файли за межі закладу, а деякі – для певних груп, створених адміністратором.

Адміністратор може створювати окремі групи працівників, батьків та за потреби поширювати документи, обираючи певні групи, а не окремих осіб.

Адміністратор (відповідальна особа) створює резервну копію найцінніших файлів, що

надає можливість виконати відновлення інформації за умов втрати оригіналу, з якого було створено резервну копію. При цьому під втратою треба розуміти настання події, що призвела до зміни даних, після чого вони втратили цінність або були видалені.

Доступ до файлів надається не тільки працівнику(ам), який(і) їх створюють чи додають, а й співробітникам, які з ними працюють.

Закладом освіти забезпечується контроль доступів.

Адміністрація закладу освіти надає та блокує доступ до найцінніших файлів.

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

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

Крім прав доступу керівник визначає відповідальних за конкретний документ та циклічність його оновлення.

Для забезпечення роботи з електронними документами та своєчасного їх виконання у закладі освіти розробляються та затверджуються схеми проходження електронних документів згідно з розпорядчими документами про розподіл обов'язків між адміністрацією закладу, посадовими інструкціями, номенклатурою справ.

Відповідно до цих схем працівникам надається доступ до електронних документів. Наприклад,

1. Прийом відповідальною особою за діловодство вхідних листів через електронну пошту закладу освіти, реєстрація у відповідному електронному журналі вхідної документації, завантаження електронного листа до електронної папки у хмарному сховищі.

2. Резолюція та надання директором закладу освіти доступу до електронного листа відповідно до повноважень між членами адміністрації.

3. Контроль за виконанням резолюції здійснює директор закладу освіти.

4. Проєкти наказів, вихідних документів реєструються відповідальним за діловодство у відповідному журналі реєстрації наказів/вихідних документів.

5. Доступ до електронних версій наказів, вихідних документів надається членам адміністрації відповідно до повноважень.

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

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

До персональних даних в системі ІСУО мають доступ директор, відповідальна особа.

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

IV РОЗДІЛ. Сайт закладу освіти

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

Сайт створюється з метою спрощення комунікації всіх учасників освітнього процесу; інформування громадськості про особливості закладу освіти, історії його розвитку, про освітні програми та проєкти тощо; для позитивної презентації інформації про досягнення вихованців та педагогічного колективу, дотримання принципу прозорості в діяльності закладу освіти та систематичне інформування учасників освітнього процесу про діяльність закладу освіти, впорядкування робочих процесів, активного впровадження інформаційно-комунікаційних технологій у практику роботи закладу освіти створення умов мережевої взаємодії закладу освіти з іншими установами.

Сайт закладу освіти функціонує відповідно до Положення про сайт закладу освіти, схвалений рішенням педради від 31.08.2023 (протокол №1), введеного в дію наказом від 31.08.2023 №88р, яким визначено мету і завдання функціонування сайту, структуру сайту, основні підходи до інформаційного наповнення сайту.

Функціонування сайту поєднує в собі процес збору, обробки, оформлення, публікації інформації з процесом інтерактивної комунікації і в той же час презентує актуальний результат діяльності закладу.

Сайт розміщено на українському сервері - http://zdo290.zp.ua/.

Конкретне доменне ім'я затверджуються наказом керівника закладу освіти.

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.

Актуальні паролі для управління сайтом з короткою інструкцією щодо їх використання зберігаються в запечатаному конверті у керівника закладу.

При кожній зміні паролів адміністратор/редактор сайту зобов'язаний виготовити новий конверт з актуальними паролями, запечатати його, поставити на конверті дату і свій підпис, та передати керівникові закладу в триденний термін з моменту зміни паролів. Керівник закладу може використати конверт з паролями для доступу до сайту при відсутності адміністратора.

При звільнені адміністратора/редактора сайту впродовж доби здійснюється зміна паролів.

При звільнені керівника закладу конверт з паролем передається виконувачу обов’язків. Пароль змінюється в штатному режимі, зокрема після призначення керівника закладу освіти.

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

Адміністрація закладу освіти (керівник закладу та 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,педагогів,вихованців, може бути розміщена на окремих сайтах, спеціалізованих сайтах, доступ до яких організовується із сайту закладу.

Забороняється розміщення на сайті закладу освіти інформації рекламно-комерційного характеру та інформації, яка не належить до сфери діяльності установи.

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

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

Для захисту сайту закладу освіти потрібно передбачити та забезпечити:

Технічний захист - це аспект безпеки, що стосуються захисту технічних 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 дотримання 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 (працівників) 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 якої 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 (умови зарахування вихованців до закладу освіти, кількість вільних місць тощо).

Перевірка та актуалізація матеріалів, розміщених на сторінках сайту, проводиться не рідше *одного разу на півріччя*.

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, допускається здійснення відео-та фотозйомки навчальних занять, розміщення цих матеріалах на офіційних ресурсах закладу освіти без зазначення персональних даних вихованців, педагогів, локації (на період дії воєнного стану).

Крім того, якщо щодо дитини або працівника 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, 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.

Частота та періодичність зміни паролів для облікових записів закладу освіти встановлюється даним положенням.

Визначено електронну пошту (ел.пошта) закладу освіти: 290nadezhda@gmail.com (адреса)

Визначається відповідальна особа за зміну паролів та налаштування додаткових параметрів облікового запису. Змінений пароль повідомляється керівнику закладу освіти (в конверті для збереження в сейфі). Пароль оновлюється за потребою.

Особиста ел.пошта використовується працівниками закладу освіти для особистого листування.

Корпоративна ел.пошта використовується для внутрішньої комунікації (між

працівниками закладу освіти), зовнішньої комунікації (з батьками здобувачів освіти, представниками громадськості, установами та організаціями тощо).

Корпоративний акаунт забезпечує безпечність інформаційного середовища; доступ до внутрішніх користувачів та створених ними матеріалами в межах домену закладу освіти; налаштування обмеженого чи тимчасового доступу для зовнішніх користувачів не з закладу освіти; відсутність реклами; захист, налаштування та відновлення персональних даних користувачів; хмарне сховище для файлів тощо.

Для здійснення адміністрування ел.пошти закладу освіти призначається один або кілька адміністраторів із правом доступу до облікових записів адміністраторів

Адміністратори корпоративної пошти також можуть мати контроль над керуванням обліковими записами, доступом до електронної пошти та іншими аспектами поштової системи. Вони забезпечують правильну роботу та підтримку інфраструктури електронної пошти в закладі освіти.

Адміністратори несуть відповідальність за підтримання конфіденційності та безпеки облікових записів кінцевих користувачів і паролів, пов'язаних із цими обліковими записами; використання облікових записів кінцевих користувачів.

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

Управління доступом передбачає:

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

Обов'язок дотримуватись правил користування корпоративною електронною поштою, акаунтом, 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.

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, Google, jimdofree.

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 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 особами додаткової (приватної) інформації стосовно особи, членів її сім'ї, колег на сторінці освітнього закладу в соціальних мережах не публікується інформація, що може поставити під загрозу особисте життя особи, життя членів її сім'ї та інших осіб; обмежується доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі; здійснюються налаштування, які найбільше захищають додаткові відомості про власника акаунта, зокрема, не зазначається геолокація (місце розташування освітнього закладу); здійснюється періодичний перегляд списку «друзів» у соціальній мережі (якщо серед них є незнайомі або підозрілі акаунти, необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу); не використовуються соціальні мережі та пошукові системи доступ до яких обмежено відповідно до Указу Президента України «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

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

Для будь-яких контактів чи комунікації між учасниками освітнього процесу закладу освіти використовуються Viber спільнота.

В закладі освіти таким засобом комунікації виступають, Viber-спільноти, для комунікації та різного роду інформування учасників освітнього процесу, класифікуються за призначенням: для інформування учасників освітнього процесу про новини закладу освіти; для спілкування педагогічних працівників з адміністрацією; для обміну інформацією між педагогом та батьками.

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

Керівник закладу освіти призначає відповідального адміністратора .

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

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

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

Адміністратор може змінювати правила спільноти відповідно до ситуації.

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

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

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

Загальні правила щодо спілкування в чатах обговорюються на засіданнях колегіального органу управління закладом освіти (педради), органів самоврядування (зокрема, 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 працівників, зокрема, й у цифровому

середовищі, важливо встановити чітку межу.

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

Комунікаційна політика закладу освіти забороняє (*обмежує*) будь-які контакти, 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 режимі, закладом освіти установлюються чіткі приписи як для співробітників, так і для здобувачів освіти (наприклад, що бажано підготувати місце для віддаленого заняття/сеансу зв'язку та подбати про тих, хто перебуває поруч – чи то вдома).

VII РОЗДІЛ. Особливості організації освітнього процесу.

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

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

Для забезпечення діяльності закладу освіти в умовах режиму дистанційного навчання в закладі освіти прийнято положення дистанційного навчання, яким узгоджено правила та алгоритми взаємодій усіх учасників освітнього процесу для виконання освітніх програм закладу в даному форматі надання освітніх послуг.

Для організації дистанційного формату навчання в закладі освіти визначено онлайн-платформу - Google Classroom, YouTube, Trello, Padlet.

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

Визначено перелік сервісів для проведення відеоконференцій та онлайн-зустрічей (*ZOOM, GoogleMeet*) в закладі освіти для здобувачів освіти різних вікових категорій.

Відповідно до Положення про академічну доброчесність (затвердженого наказом від 11.01.2023 №006р) в закладі освіти забезпечується дотримання академічної доброчесності всіма учасниками освітнього процесу.

Спільно з батьками вихованців в закладі освіти приймається рішення щодо умов проведення відеозйомки навчальних занять, публікації відеоматеріалів або творчих робіт дітей у мережі Інтернет (на сайті закладу освіти, на сторінках соцмереж).

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 онлайн, 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.

3. Плануємо та організовуємо профілактичні заходи з метою підвищення обізнаності педагогів, керівників закладів освіти, батьків та їхніх дітей.

4. У разі виявлення, що дитина стала жертвою будь-яких проявів насильства, експлуатації, вербування або маніпуляцій у цифровому просторі, інформуємо керівника закладу освіти, який приймає рішення про звернення до Національної поліції України та надсилання повідомлення про правопорушення до департаменту кіберполіції Національної поліції України. Доводимо до постраждалого інформацію про можливість отримання психологічної допомоги та підтримки.

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 .

Орієнтовна Програма просвітницької роботи з учасниками освітнього процесу.

І Просвітницькі заходи з 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 з 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 учителям та 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.	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 вихованцями.

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;

Безпека в цифровому суспільстві	Використання цифрових сервісів та технологій для: − розпізнавання та протидії маніпуляційних технологій і пропаганди, перевірки надійності джерел і достовірності даних, небезпек в цифровому просторі; − розуміння важливості відповідальної і безпечної поведінки в цифровому просторі; − уникнення ризику здоров'я і загроз для фізичного і психологічного благополуччя при роботі у цифровому просторі; − запобігання онлайн-злочинів в цифровому суспільстві; − формування вміння захистити цифрові пристрої, дані та інші ресурси; − знання заходів безпеки, розуміння персональної відповідальності кожного щодо ризиків та загроз при 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	

3.1.Добір цифрових ресурсів	При використанні цифрових сервісів: - знати цифрові ресурси, які використовуються для навчання учнів/вихованців, зокрема, ті, які добираються закладом освіти з урахуванням мети, умов навчання, віку та потреб дітей; - вміти оцінювати достовірність даних і надійність цифрових джерел і ресурсів, якими користується дитина; - дотримуватись доброчесності при використанні цифрових ресурсів (наприклад, правових і етичних норм).

5. Розробка рекомендацій батькам щодо організації комунікації з дитиною:

- говорити з дитиною про безпеку в інтернеті та допомагати розвивати критичне мислення, вчити робити аргументований вибір та нести відповідальність за його результати;
- будувати відкриті та довірливі стосунки з дитиною;
- формувати корисні звички використання ґаджетів та цифрового середовища та підвищувати самооцінку дитини, дозволяти дитині самостійно робити вибір і бути відповідальною за це;
- заохочувати користуватися ґаджетами в зонах видимості дорослих;
- встановлювати часові межі користування ґаджетами та контролювати додатки, ігри, вебсайти та соціальні мережі, якими користується дитина, та їх відповідність віку дитини;
- бути уважними до ознак страху чи тривоги, зміни поведінки, режиму сну та апетиту.
- будувати довірливі стосунки між дітьми та дорослими (педагогами, батьками, близькими людьми).

IX РОЗДІЛ. Захист персональних даних в цифровому середовищі закладу освіти

Відповідно до Закону України «Про захист персональних даних» під час прийняття на роботу працівника, зарахування здобувача освіти до закладу освіти, подання відповідної заяви батьками здобувача освіти оформлюється згода суб'єкта персональних даних (батьки здобувачів освіти, працівники закладу освіти) шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки.

Розпорядником персональних даних є заклад освіти, якому володільцем персональних даних або законом надається право обробляти ці дані від імені володільця.

Використання персональних даних закладом освіти здійснюється за умови забезпечення захисту цих даних.

Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи здійснюється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

Під час здійснення освітньої діяльності закладом освіти забезпечується дотримання визначеної ним політики цифрової безпеки, умов та правил використання цифрових технологій, мобільних та інших електронних пристроїв.

X РОЗДІЛ. Прикінцеві положення

Періодичність оновлення Положення – один раз на три роки з дати затвердження.

Порядок обговорення оновлень визначається педагогічною радою.

Оновлене Положення обговорюють на засіданні колегіального органу закладу освіти до початку навчального року, як виключення терміново - за потребою.

Будь-які порушення Положення розглядаються відповідно до обставин, у яких вони мали місце, до визначення дисциплінарних санкцій.

На період дії правового режиму воєнного стану застосовуються обмеження в публікації інформації, інших даних, визначених органами законодавчої влади, закладом освіти. Обмеження визначаються окремими наказами по закладу освіти.

Використані джерела:

РОЗДІЛ	Використані джерела
II	https://zakon.rada.gov.ua/laws/show/z0582-18#n13 https://zakon.rada.gov.ua/laws/show/3792-12#Text https://zakon.rada.gov.ua/laws/show/z0044-05#Text https://uk.wikipedia.org https://ips.ligazakon.net/document/view/KR020247?an=88
III	Курс **"**Цифрова безпека для громадських організацій в умовах війни" від "Prometheus" **https://naurok.com.ua/post/dilova-dokumentaciya-zakladu-osviti-stvorennya-dokumentiv-v-elektronniy-formi** • Закон України No2297-VI «Про захист персональних даних». • Наказ МОН України від 08.08.2022 № 707 "Про затвердження Інструкції з ведення ділової документації у закладах загальної середньої освіти в електронній формі" • Наказ МОН України від 25.06.2018 № 676 "Про затвердження Інструкції з діловодства у закладах загальної середньої освіти"
IV	**https://naurok.com.ua/polozhennya-pro-sayt-zakladu-osviti-283304.html**
VII	**https://mon.gov.ua/storage/app/media/zagalna%20serednya/metodichni%20recomendazii/2020/metodichni%20recomendazii-dustanciyna%20osvita-2020.pdf** **https://www.helsinki.org.ua/articles/orhanizatsiia-dystantsiynoi-formy-osvity-v-zzso-v-umovakh-voiennoho-stanu-na-shcho-potribno-zvernuty-uvahu/** **https://jurfem.com.ua/bezpechna-shkola-vyklyky-systemy-osvity-v-umovakh-viyny/** **https://osvita.ua/school/79806/** **https://sqe.gov.ua/yak-vchitelyu-organizuvati-svoyu-robotu-p/**

VIII	**https://docs.google.com/document/d/1iQsUdO0NeURqX907RGALd9KMFjSqYcKK/edit?usp=sharing&ouid=118285750042345711319&rtpof=true&sd=true** https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelines-for-Parents-Educators-UAfin.pdf
IX	**https://www.ombudsman.gov.ua/storage/app/media/dystantsiyna-osvita.pdf** **https://osvita.ua/school/79806/**