СХВАЛЕНО
педагогічною радою
протокол № 2 від 18.10.2023

ЗАТВЕРДЖЕНО
Директор СЗДО № 190 ЗМР
_____ Лілія СОЛОП
наказ від 18.10.2023 № 90

ПОЛОЖЕННЯ
про цифрову безпеку
спеціального закладу дошкільної освіти (ясел-садка)
№ 190 «Дюймовочка» Запорізької міської ради

I. Загальні положення

Положення про цифрову безпеку спеціального закладу дошкільної освіти (ясла-садка) №190 «Дюймовочка» Запорізької міської ради визначає політику цифрової безпеки спеціального закладу дошкільної освіти (ясла-садка) №190 «Дюймовочка» Запорізької міської ради (далі – СЗДО).

Положення про цифрову безпеку спеціального закладу дошкільної освіти (ясел-садка) №190 «Дюймовочка» Запорізької міської ради» (далі – Положення) описує основні принципи побудови системи управління інформаційною безпекою СЗДО, посадових обов'язків і практик, які використовуються СЗДО для зменшення цифрових ризиків та збереження персональних даних учасників освітнього процесу.

Положення розроблене з урахуванням вимог законів України «Про освіту», «Про повну загальну середню освіту», «Про дошкільну освіту», «Про позашкільну 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 СЗДО 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 Положенні 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;

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, визначених законодавчими актами України.

ІІ. Системотехнічне забезпечення цифрового освітнього простору

Цифровий освітній простір СЗДО складають наступні компоненти:

внутрішні: комп'ютери, цифрове діловодство;

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

Забезпеченість робочими комп'ютерами

1. Загальна кількість персональних комп'ютерів в СЗДО складає 6 (з них в робочому стані – 5, не працює – 1) .

2. Із загальної кількості у робочому стані 5 персональних комп'ютерів на 14 робочих місць.

3. В користуванні адміністрації – 3 персональних комп'ютера: з них 2 стаціонарних (методичний кабінет та кабінет сестри медичної старшої), 1 – портативний (кабінет директора), що складає 60 % від загальної кількості працюючих комп'ютерів та 75 % від робочих місць.

4. В користуванні педагогічних працівників – 2 портативних комп'ютера, що складає 40% від загальної кількості працюючих комп'ютерів та 20 % від робочих місць.

5. Наявність комп'ютерної техніки, якій більше 5 років, складає 80 % (4 шт.).

6. Кількість персональних комп'ютерів версії операційної системи Windows (7,10,11) складає 5 .

Налаштування та обслуговування комп'ютерів працівників

У закладі відсутній інженер електронник.

Відповідальна особа за цифрову безпеку у СЗДО відповідає за належне функціонування комп'ютерів у мережі закладу: налаштовує комп'ютери працівників закладу, має знання про мережеві налаштування, звертається до сервісних центрів з питань установки програмного забезпечення та його безпеки.

У деяких випадках працівники можуть самостійно налаштовувати свої особисті комп'ютери, особливо якщо вони працюють з власних пристроїв. Проте, відповідальна особа СЗДО надає настанови та рекомендації щодо необхідних налаштувань та доступів до мережі. Виконання цих налаштувань є зоною відповідальності працівників.

Щодо налаштування доступів відповідальна особа СЗДО може керувати доступами до різних ресурсів, таких як файли, папки, програми або вебсайти, налаштовує права доступу та ролі для кожного працівника.

Налаштування комп'ютерів працівників СЗДО	ПІБ відповідальної особи
Адміністратор мережі (інженер- електронік)	Відсутній
Самостійне налаштування при роботі працівника на особистому комп'ютері. Відповідальна особа проводить обов'язкове ознайомлення працівників з «Загальними настановами та рекомендаціями щодо налаштувань і доступів до мережі» .	Головко Наталія Василівна

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 бездротове 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 облікові записи для кожного працівника.

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 впроваджується вільне використання програм без виплати винагороди автору, але не передбачає можливості внесення змін у програму.

Порядок оновлення доступу при звільненні працівника

Для забезпечення цифрової безпеки в СЗДО 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/наявні в групі (кабінеті), матеріально відповідальній особі.

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

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

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

7. Відповідальна 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 СЗДО директор закладу призначає відповідальну ним особу. Уповноваженою особою в закладі з цього питання є відповідальна особа за цифрову безпеку, до функціональних обов'язків якої входить:

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 відповідальна особа 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 відповідальна особа, працівники користуються правилом складних паролів: пароль повинен містити 8 (12) і більше символів, а саме великі та маленькі літери, цифри, спеціальні символи. Пароль має бути без загальнодоступної інформації (ім'я, прізвище, нік, важливі дати, номери телефонів, ІПН, адреси тощо); 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, Bitwarden, LastPass, KeePass тощо);
- резервне копіювання для кожного способу.

Доступ до інформації та місця збереження паролів має представник адміністрації закладу (відповідальна особа).

Обслуговування комп'ютерів, які використовуються для спільної роботи, здійснюється 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. Створити журнал реєстрації щодо користуванням ПК.
4. Прописати правила користування зовнішніми носіями інформації (флеш, карти пам'яті).
5. Слідкувати за оновленнями: переконатися, що отримуються автоматичні оновлення від служби Windows Update і інсталювати всі необхідні для організації оновлення.
6. Безпечно зберігати дані. Заклад надає ресурс для зберігання даних, наприклад Google Drive 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.
8. Налаштувати наступні рівні захисту:

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

– процедурний (на процедурному рівні вживаються заходи, що реалізуються людьми; групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки).

Функціонування загальної мережі ПК в СЗДО

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

Для підключення ПК до мережі укладено договір з інтернет-провайдером Global Net, 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 та *провідний Ethernet*, а також налаштовано доступ до мережі шляхом введення облікових даних (ім'я користувача та пароль).

Загальна мережа СЗДО	
Інтернет провайдер закладу освіти	Global Net
Тип підключення закладу освіти до мережі Інтернету (бездротовий Wi-Fi або провідний Enternet)	Інтернет кабель та Wi-Fi
Налаштування доступу до мережі Інтернету закладу освіти шляхом введення облікових даних, таких як ім'я користувача та пароль	Солоп Лілія Валеріївна
Відповідальна особа закладу освіти	Головко Наталія Василівна
Встановлення рівня доступу до мережі на ПК	Рівень користувача

ІІІ. Електронне діловодство

Ведення електронного діловодства в СЗДО здійснюється відповідно до чинного законодавства, Інструкції з діловодства у спеціальному дошкільному навчальному закладі (яслах-садку) № 190 «Дюймовочка» Запорізької міської ради Запорізької області, затвердженої наказом керівника від 04.11.2021 № 157.

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 хмарного носія для роботи з документами – якою володіє та централізовано керує заклад освіти.

Найцінніші файли закладу зберігаються – на портативному комп'ютері директора СЗДО.

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.

Відповідальна особа створює працівникам облікові записи, блокує доступи, відстежує, за потреби, активність користувачів, керує налаштуваннями безпеки відповідно до вимог безпеки закладу.

Відповідальна особа може заборонити користувачам поширювати певні файли за межі закладу.

Відповідальна особа може створювати окремі групи працівників, батьків здобувачів освіти та за потреби поширювати документи, обираючи певні групи, а не окремих осіб.

Відповідальна особа створює резервну копію найцінніших файлів, що надає можливість виконати відновлення інформації за умов втрати оригіналу, з якого було створено резервну копію.

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 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.
4. Проєкти наказів, вихідних документів реєструються відповідальним за діловодство у відповідному журналі реєстрації наказів/вихідних документів та завантажуються до електронної папки у хмарному сховищі.
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.

Електронні документи передаються до електронного архіву (зберігаються в захищеному хмарному сховищі). Для передачі електронних справ на зберігання до архіву закладу освіти проводиться експертиза цінності документів.

Архівні електронні документи групуються у справи за відповідними електронними справами.

Для вилучення електронних документів з архіву складається акт про їх знищення.

До персональних даних в системі ІСУО мають доступ директор та відповідальний реєстратор.

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

IV. Офіційний вебсайт

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

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 сервері – duymovochka190.jimdo.com.

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

Керівник СЗДО призначає відповідальну особу за ведення сайту, який несе відповідальність за вирішення питань про розміщення інформації, про видалення чи оновлення застарілої інформації.

Відповідальна особа за ведення 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 директора.

При кожній зміні паролів відповідальна особа за ведення сайту зобов'язана 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.

При звільнені відповідальної особи за ведення 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.

Адміністрація СЗДО, відповідальна особа за ведення сайту, автори публікацій несуть персональну відповідальність за зміст інформації, розміщеної 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 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 СЗДО 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 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, може бути розміщена на окремих блогах та сайтах, спеціалізованих сайтах, доступ до яких організовується із сайту закладу.

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

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

Відповідальність за зміст інформації, що висвітлюється на сайті СЗДО, несе керівник закладу та особи, відповідальні за інформаційну 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 програмного 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 (адміністрації, працівників) допускаються до розміщення тільки з їх письмової згоди. Матеріали про вихованців закладу – з письмової згоди батьків або законних представників.

Заклад освіти забезпечує механізм, щоб батьки здобувачів освіти або особи, які їх замінюють, мали безстрокове право скасувати свою згоду на обробку особистих даних дитини, вимагати виправлення неточної, неповної, застарілої інформації про неї, знищення інформації про вихованців, 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 контенту з порушенням авторських прав та умов ліцензування, контрафактних аудіо-, фото- та відеоматеріалів, примірників програмного забезпечення та посилання на такі матеріали.

Всі учасники освітнього процесу повинні бути проінформовані про механізми надання допомоги та послуги підтримки, а також про процедури подання скарг, поновлення прав або відшкодування, якщо їхні права порушуються на сайті закладу.

Інформація про права людини та права дитини в цифровому середовищі розміщується на сайті закладу 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 є офіційним портфоліо закладу освіти.

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

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

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.

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

Крім того, якщо до 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.

СЗДО 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 заняття, пам'ятки, рекомендації тощо), розроблені працівником закладу, розміщується на сайті закладу освіти з інформацією про автора.

В разі використання на сайті закладу 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. Засоби зовнішньої комунікації (електронна пошта закладу)

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

Електронна пошта для СЗДО 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: duymovochka190@ukr.net .

Відповідальна особа за цифрову безпеку відповідає зміну паролів та налаштування додаткових параметрів облікового запису. Змінений пароль повідомляється директору СЗДО (в конверті для збереження в сейфі). Пароль оновлюється один раз на пів року.

Особиста ел.пошта використовується працівниками СЗДО для особистого листування.

Корпоративна ел.пошта використовується для внутрішньої комунікації (між працівниками закладу), зовнішньої комунікації (з батьками здобувачів освіти, представниками громадськості, установами та організаціями тощо).

У разі звільнення працівника чи вибуття здобувача освіти, електронна скринька таких користувачів ліквідовується.

Працівник закладу не має права:

а) використовувати електронну пошту СЗДО для цілей, не пов’язаних з виконанням посадових обов’язків в закладі;

б) повідомляти пароль доступу до адреси скриньки іншим особам;

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

г) розсилати листи, що містять:

- конфіденційну інформацію, доступ до якої обмежено чинним законодавством, у тому числі містить державну таємницю, матеріали, використання яких порушує права власності;
- недостовірну інформацію, а також інформацію, що ображає честь і гідність осіб, ганьбить ділову репутацію, пропагує ненависть або дискримінацію людей за расовими, етнічними, статевими, релігійними, соціальними ознаками, закликає до протиправних дій;
- матеріали, що містять віруси або інші комп’ютерні коди; файли, програми, призначені для порушення, знищення або обмеження функціональності будь-якого 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, акаунтом, наданим закладом освіти, вноситься до посадових обов’язків працівника.

VI. Засоби зовнішньої комунікації (соціальні мережі, месенджери)

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

Інформаційна відкритість забезпечується наявністю у СЗДО 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 СЗДО мережева комунікація здійснюється в Facebook, Viber та YouTube.

Керівник закладу призначає відповідальну особу, яка несе відповідальність за оприлюднення достовірної, точної та повної інформації, а також у разі потреби перевіряє правильність та об'єктивність наданої інформації і оновлює оприлюднену інформацію.

Відповідальна особа (адміністратор сторінки) СЗДО 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 (у т.ч. із застосуванням сервісів VPN), 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 використовуються спільноти в месенджері.

У СЗДО таким засобом комунікації виступають Viber-спільноти.

Спільноти, сформовані для комунікації та різного роду інформування учасників освітнього процесу, класифікуються за призначенням: для інформування учасників освітнього процесу про новини закладу; для спілкування педагогічних працівників з адміністрацією; для обміну інформацією між педагогами та батьками вихованців та інші.

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

Відповідальною особою за цифрову безпеку здійснюється ведення спільноти закладу.

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 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 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), інших органів самоврядування.

Правила спілкування в чатах

– *Поважайте чужі часові рамки, бережіть особистий час. Встановіть та дотримуйтесь часових обмежень для надсилання повідомлень(не писати у чат після 19:00).*

– *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 СЗДО розуміння ризиків втрати онлайн-репутації – власної та закладу.

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

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

Комунікаційна політика закладу освіти обмежує будь-які контакти, не пов'язані з освітньою діяльністю, та контакти на платформах, що не мають стосунку до закладу.

На випадок проведення відеоконференцій або занять у віддаленому режимі, закладом освіти установлюються чіткі приписи як для співробітників, так і для здобувачів освіти (що бажано підготувати місце для віддаленого заняття/сеансу зв'язку та подбати про тих, хто перебуває поруч).

VII. 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.

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 про дистанційне навчання у СЗДО № 190 ЗМР (наказ від 30.098.2023 № 70), 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-платформи Zoom, GoogleMeet, віртуальна дошка 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 для учасників освітнього процесу.

З метою захисту персональних даних під час дистанційного навчання забезпечується дотримання вимог щодо захисту персональних даних учасників освітнього процесу в електронному освітньому середовищі.

В разі використання під час дистанційного навчання особистих домашніх пристроїв, які зазвичай не охоплюються мережевим захистом, проводиться робота щодо ознайомлення вихователів та батьків вихованців з необхідністю перевірки надійності інтернет-провайдера, а також системна робота з навчання всіх учасників освітнього процесу правилам поведінки в інтернеті для забезпечення безпеки учасників освітнього процесу, зокрема, шляхом системної роботи з розвитку цифрової грамотності; надання рекомендацій щодо встановлення на всіх пристроях брандмауера та антивірусних програм, батькам – за необхідності – програм фільтрації, блокування або відстеження, використання контент-фільтрів (системи батьківського контролю) і безпечних пошукових систем або обмежень доступу, щоб фільтрувати контент, який діти можуть переглядати в інтернеті.

Організовано ознайомлення учасників освітнього процесу з політикою закладу освіти, що регулює використання інформаційних технологій (сервісів, ресурсів) різними учасниками освітнього процесу. На початку навчального року (протягом року за необхідності) педагогами проводиться обов'язкове ознайомлення батьків з переліком ресурсів, які використовуватимуться в навчанні, надаються інструкції до роботи з вказаними з цифровими інструментами, створюються стислі пам'ятки щодо роботи, відеоінструкції тощо.

Закладом освіти проводяться заходи щодо дотримання авторського права.

Відповідно до Положення про академічну доброчесність (затвердженого наказом від 18.10.2023 № 90) в СЗДО 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, в блогах, на сторінках соцмереж).

В закладі освіти визначено порядок реагування працівників на інциденти, пов'язані з безпекою дітей, зокрема в цифровому середовищі:

- негайне інформування відповідальної особи або керівника закладу про інцидент, пов'язаний з безпекою дітей, що виник в цифровому середовищі, для прийняття рішення щодо подальших дій: інформування батьків дитини, відповідних служб та установ правопорядку про встановлені порушення прав дитини;
- збереження (фіксація) ознак інциденту, у тому числі на матеріальних носіях;
- забезпечення захисту інформаційних ресурсів закладу освіти;
- проведення, за потреби, відповідної профілактичної роботи з учнями.

В закладі освіти прийнято правила (вимоги) проведення дистанційного (онлайн) заняття: визначені умови підключення до онлайн-заняття; правила поведінки; використання мікрофону та камери; правила використання чату, спілкування в чаті; рекомендації до зовнішнього вигляду учасників освітнього процесу, застосування фонових зображень тощо.

Про дотримання цих правил інформуються всі учасники освітнього процесу.

Використання технічних засобів навчання та мобільних пристроїв (ноутбуків, планшетів, смартфонів) під час дистанційного навчання є базовою умовою для організації освітнього процесу засобами цифрових технологій. СЗДО проводиться робота з інформування учасників освітнього процесу щодо забезпечення безпеки пристроїв під час навчання.

VIII. Проведення заходів просвітницького характеру

З метою дотримання права дитини на безпеку та захист, яке є базовим та поширюється на її життєдіяльність як офлайн, 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 здійснюються наступні кроки:

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

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

3. Плануються та організовуються профілактичні заходи з метою підвищення обізнаності педагогів, адміністрації закладу, батьків вихованців.

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

Відповідальна особа за цифрову безпеку проводить роботу з питань просвіти учасників освітнього процесу.

За відповідними напрямками складається Програма просвітницької роботи (або план проведення просвітницьких заходів на навчальний рік) для всіх категорій учасників освітнього процесу (цей документ може бути прийнятим та затвердженим окремо від даного Положення, може бути складовою даного Положення).

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.

Проведення заходів відповідно до Програми (Плану заходів) просвітницької роботи здійснюється відповідальної особою за цифрову безпеку, призначеною керівником закладу, та педагогічними працівниками під час проведення занять, батьківських зборів тощо.

До проведення заходів просвітницького характеру в закладі можуть залучатись за згодою фахівці в сфері інформаційно-комунікативних технологій, правозахисту, громадські організації, підприємства.

До Програми (Плану заходів) просвітницької роботи можуть вноситися зміни з урахуванням динамічного розвитку цифрових технологій та відповідно до актуальних потреб учасників освітнього процесу.

Програма просвітницької роботи з учасниками освітнього процесу СЗДО.

І. Заходи просвітницького характеру з педагогічними працівниками 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 пам'яток, брошур або інших матеріалів про цифрову безпеку, які освітяни можуть використовувати в своїй роботі 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 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.	
4	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.	Згідно листа МОНУ №1/9-128 від 10.03.2021 «Щодо необхідності проведення додаткових профілактичних заходів в середовищі дітей та підвищення обізнаності батьків».

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

Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки включають формування цифрових компетентностей для навчання та життя, ознайомлення з основами кібербезпеки, правилами безпечної роботи в Інтернеті.

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 дозволу у батьків (діти 4-6 років).*

2. Відповідно до отриманих результатів щодо рівня умінь дітей дотримуватись правил безпечної поведінки в цифровому просторі визначення напрямків/відповідних заходів просвітницького характеру з вихованцями.

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

№ з/п	Просвітницькі заходи	Примітки
1.	Проведення занять, бесід, інших видів діяльності на тему важливості поваги до інших людей в онлайн-середовищі та спільного створення позитивного і безпечного інтернет-середовища.	Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
2.	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; – розміщення пам'яток з правилами безпечної поведінки в Інтернеті, на видимих місцях у закладах освіти; створення плакатів, які діти можуть легко розуміти і запам'ятовувати;	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

III. 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.

№ з/п	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: − 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.
1.4	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 із закладом освіти		
2.1	Комунікація. Використання цифрових сервісів	Використання цифрових сервісів для: − участь у онлайн-заходах для спілкування з закладом освіти, дотримання, наприклад, правил зустрічі, заходів тощо;

	для покращення комунікації батьків із закладом освіти або третіми особами. Розвиток співпраці та вдосконалення організаційних стратегій комунікації	− 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 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 як правило 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.