ПОГОДЖЕНО
на загальних зборах (конференції)
закладу освіти

протокол від 31.08.2023 №1

СХВАЛЕНО
на засіданні педради закладу освіти

протокол від 31.08.2023 №1

ЗАТВЕРДЖЕНО
наказом від 31.08.2023 №51/р

ЗАКЛАД ДОШКІЛЬНОЇ ОСВІТИ (ЯСЛА-САДОК) №290 «ЗАЙЧАТКА» ЗАПОРІЗЬКОЇ МІСЬКОЇ РАДИ

ПОЛОЖЕННЯ
«Про цифрову безпеку закладу дошкільної освіти №290 «Зайчатка» Запорізької міської ради»

м. Запоріжжя

2023

Зміст

I РОЗДІЛ. Загальні положення

Положення «Про цифрову безпеку закладу дошкільної освіти №290 «Зайчатка» Запорізької міської ради» визначає політику цифрової безпеки закладу дошкільної освіти №290 «Зайчатка» Запорізької міської ради (далі ЗДО №290 ЗМР) .

Положення «Про цифрову безпеку закладу дошкільної освіти №290 «Зайчатка» Запорізької міської ради» (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 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 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 Положенні нижченаведені 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;

блог, блоґ – мережевий журнал чи щоденник подій, що створюється на відповідних платформах для розміщення інформації, створення умов для її обговорення;

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;

сайт або **вебсайт** - сукупність вебсторінок та відповідного вмісту, доступних у мережі Інтернет, які об'єднані як за змістом, так і за навігацією під єдиним доменним ім'ям;

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 в закладі освіти складає 5 (з них в робочому стані - 4, не працюють - 1 *(відповідно до показника рядка 6100 розділу VI)*.

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

3. В користуванні адміністрації – 3 персональних комп'ютери.

4. В користуванні педагогічних працівників – 1 персональний комп’ютер.

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

уНалаштування та обслуговування комп’ютерів працівників

В закладі освіти працівники самостійно налаштовують свої особисті комп'ютери, особливо якщо вони працюють з власних пристроїв. Виконання цих налаштувань є зоною відповідальності працівників (розробляються «Загальні настанови та рекомендації щодо налаштувань і доступів до мережі»).

Щодо налаштування доступів, адміністратор мережі 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 ЗО	ПІБ відповідальної особи
Самостійне налаштування при роботі працівника на особистому комп’ютері. Обов’язкове ознайомлення працівників з «Загальними настановами та рекомендаціями щодо налаштувань і доступів до мережі»	Кравченко Т.В. Бєла Ю.В. Пасько С.О. Куценко В.С.

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.

3. *Захист від шкідливих програм.*

Встановіть надійне антивірусне програмне забезпечення та антивірусні програми.

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

Уникайте відкриття підозрілих посилань або вкладень в електронних листах.

4. *Налаштування мережі:*

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

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

5. *Настройки файрволу:*

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

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

6. *Керування обліковими записами:*

Створюйте окремі облікові записи користувачів для кожного працівника та надавайте їм відповіді.

Ліцензійне програмне забезпечення

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

У закладі освіти використовується наступне програмне забезпечення:

1) З комерційною ліцензією – передбачає, що користувач оплачує вартість використання даної програми на одному чи кількох зазначених у ліцензії комп'ютерах, серед них є:

а. «коробкові» версії ліцензії містять носій, на якому записана програма та інструкція до її використання разом з ключем для встановлення, а саме:_____

б. ЕОМ (англійська Original equipment Manufacturer - оригінальний виробник обладнання) – ліцензія, що надається на один екземпляр програми разом з певним комп'ютерним обладнанням, наприклад з ноутбуком, підтвердженням ліцензії є спеціальна наклейка, а саме:_____

в. корпоративна ліцензія – ліцензія на кілька копій програми для використання, а саме: _____.

2) Пробна або trial ліцензія на комерційне ПЗ, яка надається для пробного використання програми протягом певного часу або на певну кількість запусків програм: _____.

3) Вільного використання або freeware (freeware - вільний товар) – ліцензія передбачає вільне використання програм без виплати винагороди автору, але не передбачає можливості внесення змін у програму: _____.

4) З відкритим кодом або Free (вільний) Software чи libre (вільний) Software – ліцензія на вільне програмне забезпечення, що передбачає не тільки безкоштовне використання програм але і право на їх модифікацію, внесення змін у програму: _____

Уповноважена особа створює перелік програмного забезпечення, що використовується у ЗДО згідно з типом ліцензій.

Порядок оновлення доступу при звільненні працівника

Для забезпечення цифрової безпеки в 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/наявні в кабінеті, вихователю-методисту (уповноваженій особі).
4. Інженер-електронік (за його відсутності - уповноважена особа) має оглянути пристрої, якими користувався працівник, що звільняється, впевнитись в їх справності/сшкти 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 освіти, платформа для дистанційного навчання), ключі шифрування, паролі до роутера і т.п.).

При зміні технічного обладнання уповноважена особа (особи) контролює (-ють) 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, Bitwarden, LastPass, KeePass тощо);
- текстовий документ – зберігається документ в архіві під паролем;
- резервне копіювання для кожного способу.

Доступ до інформації та місця збереження паролів має представник адміністрації закладу освіти, керівник закладу освіти.

Обслуговування комп'ютерів, які використовуються для спільної роботи (у методичному кабінеті тощо) 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 спільної мережі Wi-Fi.
3. Створити журнал реєстрації щодо користуванням ПК.
4. Налаштувати сканер безпеки на ПК. Налаштовувати брандмауер (фаєрвол): виявляє та блокує мережевий трафік на основі попередньо визначених або динамічних правил.
5. Прописати правила користування зовнішніми носіями інформації (флеш, карти пам'яті).
6. Слідкувати за оновленнями: переконатися, що отримуються автоматичні оновлення від служби Windows Update і інсталювати всі необхідні для організації оновлення.
7. Заборонити інсталювати програмне забезпечення з-поза меж організації, яке не затверджено або не адмініструється у закладі.
8. Безпечно зберігати дані. Заклад надає ресурс для зберігання даних, як-от Google Drive або інше корпоративне сховище. Не зберігати дані лише на локальному комп'ютері.

9. Постійно нагадувати (створювати пам’ятки, викладати їх на видне місце) щодо правил безпеки.

І. Створити робочі групи в локальній мережі (наявність сервера, використання спеціалізованого ПЗ). *Наприклад, у локальній мережі закладу освіти в одну групу об’єднано комп’ютери кабінетів інформатики, в іншу групу - ПК адміністрації.*

ІІ. Створити групи в хмарному середовищі.

Наприклад, Google Workspace for Education – пакет спеціалізованого хмарного програмного забезпечення й інструментів для спільної роботи від компанії Google: усі працівники та здобувачі освіти мають корпоративні акаунти, що надає додатковий захист та безпеку (на відміну від готового спеціалізованого програмного забезпечення для офісів - у хмарному пакеті G Suite дані користувачів зберігаються не на традиційних внутрішніх серверах компаній, а в мережі захищених центрів обробки даних Google. Також перевагою є те, що дані та інформація зберігаються миттєво, а потім синхронізуються з іншими центрами даних для резервного копіювання. На відміну від безкоштовних споживчих послуг, користувачі G Suite не бачать реклами під час використання цих додатків, а інформація та дані в облікових записах G Suite не використовуються для цілей реклами. Крім того, адміністратори G Suite можуть самостійно налаштувати необхідні параметри безпеки та конфіденційності.)

ІІІ. 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);

7) процедурний (на процедурному рівні вживаються заходи, що реалізуються людьми; групи процедурних заходів: управління персоналом,

фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт).

Використання специфічних програм

Вивчення та удосконалення можливостей існуючого програмного забезпечення призвело до ефективного його використання в адмініструванні, корекційній діяльності та освітньому процесі в цілому.

В закладі освіти дозволено встановлення програм, які можуть використовуватись всіма педагогічними працівниками для віддаленого доступу до робочого столу та дій для обслуговування комп'ютера відповідальною особою і в сервісних цілях: TeamViewer, AnyDesk, Ammyy Admin, AeroAdmin, LiteManager, RAdmin.

Використання комп'ютерних програм в навчанні дітей з особливими освітніми потребами дозволяє значно покращити процес корекційного навчання за рахунок індивідуалізації процесу виконання завдання, досягнення високої мотивації. Такий підхід надає можливість подавати відповідну кількість навчального матеріалу кожній дитині у групі, враховуючи індивідуальні труднощі, швидкість виконання завдання, характер та ступінь допомоги, яку потребує здобувач освіти в процесі навчання. Типовим переліком допоміжних засобів для навчання (спеціальних засобів корекції психофізичного розвитку) осіб з особливими освітніми потребами, які навчаються в закладах освіти, затвердженого наказом Міністерства освіти і науки України від 23.04.2018 № 414 (https://zakon.rada.gov.ua/laws/show/z0582-18#n13), визначено комп'ютерні програми для ведення корекційної дільності з дітьми відповідно до нозології та їх специфічного порушення.

Орієнтовний уніфікований перелік комп'ютерних програм для дітей з особливими освітніми потребами:

Спеціалізовані програми для вивчення елементів житла родини, будови тіла людини, життя на Землі, емоцій людини, явищ природи, інш.

Спеціалізовані ігри для розвитку логіки.

Логопедична програма для корекційної роботи.

Програмно-апаратний комплекс для інтеграції абстрактної концепції з конкретними елементами.

Програма для комунікації (спілкування озвученими картинками) з порушенням опорно-рухового апарату, інтелектуальними порушеннями, сенсорними порушеннями (зниженим зором чи слухом та сліпих чи глухих).

Комплекси для розвитку мовленнєвої діяльності, для колективної роботи.

Комплекс для корекційно-розвиткової роботи.

Програма екранного доступу.

Синтезатор українського мовлення.

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 (*DSL, оптичне волокно або бездротові технології*).

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

На ПК встановлено тип підключення до мережі – бездротовий Wi-Fi (*або провідний Ethernet*), а також налаштовано доступ до мережі шляхом введення облікових даних (ім'я користувача та пароль). *Встановлення рівня доступу до мережі може також залежати від налаштувань мережевого обладнання (маршрутизатори або комутатори), які керують мережевим трафіком і можуть вимагати авторизації для підключення до мережі.*

Загальна мережа закладу освіти	Назва, відповідальна особа
Інтернет провайдер закладу освіти	LINET
Тип підключення закладу освіти до мережі Інтернету (бездротовий Wi-Fi або провідний Internet)	провідний Internet
Налаштування доступу до мережі Інтернету закладу освіти шляхом введення облікових даних, таких як ім’я користувача та пароль	вихователь-методист
Адміністратор мережі закладу освіти	вихователь-методист
Встановлення рівня доступу до мережі на ПК	вихователь-методист

ІІІ РОЗДІЛ. Електронне діловодство закладу освіти

Ведення електронного діловодства в закладі освіти здійснюється відповідно до чинного законодавства та регламентується примірною інструкцією з діловодства у дошкільних навчальних закладах (наказ МОН 01.10.2012 № 1059): ті пункти, що не суперечать ДСТУ 4163:2020 та Наказу Мін’юсту від 18.06.2015 № 1000/5.

Термін зберігання документів визначено 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 – *Dropbox*,

Mega, Microsoft One Drive, Google Drive на корпоративній платформі *Google, Microsoft 365, Slack, Trello, Asana* .

Найцінніші файли закладу зберігаються в хмарному сховищі, на спільних дисках в домені закладу.

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/люди, призначена/призначені наказом керівника закладу освіти.

Додатковим адміністратором, на випадок відсутності/недоступності основного адміністратора, має бути керівник (заступник керівника) закладу освіти.

Користувачі з правами адміністратора створюють працівникам облікові записи, блокують доступи, відстежують, за потреби, активність користувачів, керують глобальними налаштуваннями безпеки відповідно до вимог безпеки закладу. *Наприклад, адміністратор може надати пароль користувачеві, якщо той його забув, або має можливість увімкнути двофакторну автентифікацію для всіх працівників та налаштувати додатковий захист організаційного простору.*

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

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

Захист найважливішої інформації на корпоративній платформі розпочинається із облікового запису адміністратора, який має максимальні доступи. Крім захисту акаунта адміністратора та акаунтів членів адміністрації, які мають додаткові доступи, здійснюється додаткове налаштування безпеки для працівників.

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.

Керівник закладу освіти розробляє чекліст з відповідними правами доступу різних груп, що надає можливість цим групам мати доступ до спільних файлів, листування і обмежить доступ іншим групам, користувачам.

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 (офісним службовцем) 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 (офісним службовцем) у відповідному електронному 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.

За ведення даних документів відповідає куратор закладу освіти в ІСУО, який надає доступ педагогічним працівникам.

До персональних даних в системі ІСУО мають доступ директор, діловод.

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 р. (протокол № 1), введеного в дію наказом від 31.08.2023 р. № **107**/р, 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 ЗДО.

Сайт розміщено на українському сервері – https://zdo-no-29061.cms.webnode.com.ua/

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

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

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

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

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

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

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

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

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

Відповідно до Закону України «Про засади запобігання та протидії дискримінації в Україні» на сайті закладу освіти повинні бути відсутні вияви дискримінації, щодо віку, раси, кольору, статі, мови, релігії, політичних або

інших переконань учасників освітнього процесу, національного, етнічного або соціального походження, майна, інвалідності, народження або іншого статусу.

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

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

- інші інформаційні матеріали, які заборонені законодавством України.

Частина інформаційного ресурсу, який формується за ініціативи підрозділів, творчих колективів, педагогів, може бути розміщена на окремих блогах та 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 (керівників, вихователів, працівників, вихованців) 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.

Сайт має містити підтвердження права третіх осіб на вільне поширення, використання та переробку інформаційних матеріалів у вигляді повідомлення: «Весь контент доступний на умовах ліцензії CommonsAttribution 4.0 Internationallicense, якщо не зазначено інше», у разі ж, якщо викладена інформація має інші умови розповсюдження (наприклад, текстові, фото-, чи відеоматеріали, авторські права на які належать третім особам), то під такими матеріалами необхідно зробити про це відповідну ремарку.

На сайті має бути розміщена інформація щодо відповідних засобів правового захисту, в тому числі про те, як і кому подавати скаргу, повідомляти про зловживання або просити про допомогу й консультування під час користування Інтернетом, зокрема, під час користування сайтом закладу освіти.

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 освіти.

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 *(наприклад, оновлення інформації про територію обслуговування закладу 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.

Вимога про згоду на зйомку особи передбачена Конституцією України (частина 2 статті 32), Законом України «Про інформацію» (частина 2 статті 21) та Цивільним кодексом України.

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.

Батьки учня надають згоду на зйомку дітей під час освітнього процесу в закладі освіти, розміщення фото-, відеоматеріалів на офіційних порталах закладу освіти.

Після надання згоди на зйомку дитини батьки можуть вимагати припинити публічний показ (вилучити певні зображення з публічного доступу) тієї частини, яка стосується особистого життя дитини.

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

З урахуванням обмежень, визначених законодавством, допускається відкрита зйомка на вулиці, на публічних заходах, здійснення відео- та фотозйомки навчальних занять, розміщення цих матеріалах на офіційних ресурсах закладу освіти без зазначення персональних даних вихованців, вихователів, локації (останнє – на період дії воєнного стану).

Крім того, якщо щодо дитини або вихователя вчиняються протиправні дії і зйомка ведеться з метою їх фіксації, така зйомка може визнаватися допустимою, враховуючи положення частини 2 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.

З метою дотримання авторського права матеріали (наприклад, відеозапис або презентація заняття, 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 наказом керівника закладу освіти *(або даним Положенням).*

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

В разі функціонування кількох електронних скриньок (для зовнішнього листування, для внутрішньої комунікації) – зазначити перелік.

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 один раз на квартал.

Закладом освіти визначається режим використання корпоративних та особистих акантів, встановлюються правила використання поштових скриньок для співробітників.

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).

Корпоративна пошта забезпечує зручний та організований спосіб комунікації всередині установи.

Для здобувачів освіти, як правило, створюється корпоративний обліковий запис.

Корпоративний обліковий запис створюється адміністратором закладу освіти. Доступ до окремих продуктів і сервісів в корпоративному акаунті надає адміністратор (налаштування цих сервісів відрізняється для всіх учасників

освітнього процесу, окремо налаштовується облікові записи для вихователів, адміністрації).

Корпоративний акант 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.

Закладом освіти визначаються правила використання корпоративної електронної пошти, яка передбачає встановлення обов'язкових норм щодо використання, обмежень і конфіденційності інформації, використання зовнішніх поштових сервісів, обмеження відправки конфіденційних даних та використання шкільної пошти для особистих цілей тощо.

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

Використання спільних облікових записів (одночасно використовуються багатьма працівниками) в закладі освіти може бути доречним, наприклад, для загальних поштових скриньок, які призначені для спільної комунікації або отримання повідомлень від батьків.

Для здійснення адміністрування ел.пошти закладу освіти призначається один або кілька адміністраторів із правом доступу до облікових записів адміністраторів (вирішує заклад освіти, в залежності від кількості учасників навчального процесу).

Призначається адміністратор(-и) для налаштування доступу до окремих продуктів і сервісів (супровід).

Адміністратор створює корпоративний обліковий запис для кожного учасника закладу освіти та пароль (з урахуванням рекомендацій для створення надійних паролів), який користувач може змінити на власний (за бажанням).

Адміністратор корпоративної пошти забезпечує правильну роботу та підтримку інфраструктури електронної пошти в закладі освіти, також може здійснювати контроль над керуванням обліковими записами, доступом до електронної пошти та іншими аспектами поштової системи.

Адміністратор несе 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. Створення ідентифікаційних облікових записів для кожного працівника, щоб забезпечити індивідуальний доступ до електронної пошти.
2. Запровадження рівневого доступу на основі потреб та ролей працівників. Наприклад, хто має право на адміністрування системи, хто може мати доступ до конфіденційної інформації тощо.
3. Шифрування:

- використання шифрування для захисту важливої інформації, що передається через електронну пошту. Шифрування допоможе запобігти несанкціонованому доступу до конфіденційної інформації. Рекомендовано встановити TLS (TransportLayerSecurity) для шифрування передачі даних між поштовим сервером та клієнтськими пристроями.

- двофакторна аутентифікація: активація двофакторної аутентифікації для облікових записів корпоративної пошти забезпечить додатковий захист облікового запису.

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

5. Створення паролів:

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

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

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

Рекомендації щодо процесів оновлення паролю:

- регулярність: оновлення паролів на облікові записи електронної пошти *щонайменше* раз на 3-6 місяців.

- складність: пароль повинен бути складним і містити комбінацію великих і малих літер, цифр і спеціальних символів (мінімум 8 символів).

унікальність: використання унікального паролю для кожного облікового запису. Заборона використовувати один і той же пароль для різних сервісів.

Рекомендації щодо процесів архівації інформації:

- регулярність: архівування електронної пошти зі збереженням резервних копій на надійних зовнішніх носіях (*або в хмарному сховищі*) відбувається один раз на _____ *(або щомісяця до 30 числа).*

- зберігання: визначено тривалість зберігання архівних копій відповідно до політики установи та вимог щодо зберігання даних: збереження здійснюється протягом календарного року (*навчального року).*

- захист: забезпечення безпеки архівних копій шляхом використання шифрування для захисту від несанкціонованого доступу.

7. Необов'язкові додаткові заходи безпеки: використання двофакторної аутентифікації (2FA) для підвищення рівня безпеки облікового запису (може включати використання одноразових паролів, кодів підтвердження через SMS або використання аутентифікаційних додатків).

Зобов’язання користувачів корпоративної електронної пошти закладу освіти визначається закладом освіти.

Працівники закладу освіти зобов’язані використовувати корпоративну електронну пошту при здійсненні своїх посадових обов’язків, зокрема,

відправляти та отримувати електронне листування внутрішнім і зовнішнім кореспондентам з використанням адреси робочої пошти.

Працівник закладу освіти не має права:

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

б) повідомляти пароль доступу до адреси скриньки іншим особам;

в) здійснювати масову розсилку листів зовнішнім адресатам, в тому числі 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, акантом, наданим закладом освіти, вноситься до посадових обов'язків працівника.

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

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

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

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

В закладі освіти мережева комунікація здійснюється в Facebook, YouTube, Google.

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

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

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

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

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

З метою недопущення отримання зацікавленими 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 аканта, 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 освіти використовуються шкільні спільноти в месенджері.

В закладі освіти таким засобом комунікації виступають Telegram-спільноти, Viber-спільноти.

Спільноти, сформовані 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 вихователем та батьками групи .

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

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

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.

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. Працівники закладу освіти мають усвідомлювати ризики втрати онлайн-репутації – власної та закладу освіти.

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

Для будь-яких контактів між співробітниками закладу освіти та учнями/вихованцями та/або батьками в закладі освіти використовується корпоративна (офіційна) електронна пошта або аканти, створені для здійснення робочих завдань для кожного працівника.

Для безпеки педагогів створюється окремий обліковий запис або окремий користувач, якщо пристроєм – комп’ютером, ноутбуком, планшетом – вдома чи на роботі користується кілька користувачів, розмежовуються власні електронні скриньки для особистого користування та акаунт 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.

На випадок проведення відеоконференцій або занять у віддаленому режимі, закладом освіти установлюються чіткі приписи як для співробітників, так і для здобувачів освіти .

В разі звільнення працівника відповідальна особа в термін не пізніше 5 робочих днів після звільнення працівника змінює пароль доступу до акаунту закладу.

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 Стратегію (*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.

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.

Встановлено порядок та сервіси для комунікації учасників освітнього процесу: відправлення повідомлень через месенжери, в сервісі Google Classroom, за допомогою електронної пошти, тощо

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

Педагогами обговорюється використання окремих цифрових ресурсів, інтернет-платформ для створення тестів, інтерактивних завдань, іншого навчального контенту.

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

Організовано ознайомлення учасників освітнього процесу з політикою закладу освіти, що регулює використання інформаційних технологій (сервісів, ресурсів) різними учасниками освітнього процесу.

З метою ознайомлення батьків вихованців з інтерактивними технологіями, які використовуватимуться вихователем, створюються стислі пам’ятки щодо роботи в ресурсі або з цифровим інструментом.

Закладом освіти проводяться заходи щодо дотримання авторського права.

Відповідно до Положення про академічну доброчесність в закладі освіти забезпечується дотримання академічної доброчесності всіма учасниками освітнього процесу, зокрема, умов використання штучного інтелекту в освітньому процесі.

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).

Адміністрацією закладу освіти здійснюється *вибірковий* аналіз змісту навчальних матеріалів, які розробляються вихователями для занять в синхронному та асинхронному режимах, на предмет відповідності контенту навчальній програмі, віковим особливостям вихованців, дотримання етичних норм тощо.

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 освіти 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 т.ч на матеріальних носіях;
- забезпечення захисту інформаційних ресурсів закладу освіти.

Визначено відповідальну особу за розгляд інцидентів, пов’язаних з онлайновою безпекою, та організацію відповідної просвітницької роботи.

В закладі освіти прийнято правила (вимоги) проведення дистанційного (онлайн) заняття: визначені умови підключення вихованців до онлайн-заняття; правила поведінки на занятті; використання мікрофону та камери вихованцями; правила використання чату, спілкування в чаті під час онлайн-заняття.

Про дотримання цих правил інформуються всі учасники освітнього процесу.

В закладі освіти встановлюються умови та правила використання мобільних технологій та інших електронних пристроїв під час навчальних занять (*даним Положенням або окремим документом*).

Використання технічних засобів навчання та мобільних пристроїв (ноутбуків, планшетів, смартфонів) під час дистанційного навчання є базовою умовою для організації освітнього процесу засобами цифрових технологій.

Закладом освіти проводиться робота з інформування учасників освітнього процесу щодо забезпечення безпеки пристроїв під час навчання.

VIII 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.

IX 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	https://prometheus.org.ua/course/course-v1:Prometheus+DSPO101+2023_T1 https://naurok.com.ua/post/dilova-dokumentaciya-zakladu-osviti-stvorennya-dokumentiv-v-elektronniy-formi
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/

Прошнуровано, пронумеровано та скріплено печаткою 31
тридцять одне аркушів.
В.о. директора ЗДО №290 ЗМР
Тетяна КРАВЧЕНКО