

ЗАПОРІЗЬКА ГІМНАЗІЯ № 41 ЗАПОРІЗЬКОЇ МІСЬКОЇ РАДИ

ПОГОДЖЕНО

загальні збори (конференція) закладу
освіти

протокол від 29.01.2024 № 1

СХВАЛЕНО

на засіданні педради закладу освіти

протокол від 29.01.2024 № 4

ЗАТВЕРДЖЕНО

наказом від 29.01.2024 № 11

ПОЛОЖЕННЯ

Про цифрову безпеку закладу освіти

Запорізької гімназії №41 Запорізької міської ради

Запорізької області

м. Запоріжжя

2024

Зміст

I РОЗДІЛ. Загальні положення	3
II РОЗДІЛ. Системотехнічне забезпечення цифрового освітнього простору закладу освіти.....	5
III РОЗДІЛ. Електронне діловодство закладу освіти	9
IV РОЗДІЛ. Сайт закладу освіти	122
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.	133
V РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (ел. пошта закладу освіти)	15
VI РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (соціальні мережі, месенджери).....	16
VII РОЗДІЛ. Особливості провадження освіти, дистанційної освіти	19
Організація освітнього процесу. Особливості дистанційної освіти	19
VIII РОЗДІЛ. Проведення заходів просвітницького характеру	22
IX РОЗДІЛ. Захист персональних даних в цифровому середовищі закладу освіти	34
X РОЗДІЛ. Прикінцеві положення	34
Використані джерела:	35

ПОЛОЖЕННЯ

Про цифрову безпеку

Запорізької гімназії № 41 Запорізької міської ради

І РОЗДІЛ. Загальні положення

Положення «Про цифрову безпеку закладу освіти» визначає політику цифрової безпеки закладу освіти Запорізька гімназія № 41 Запорізької міської ради (далі – ЗО № 41).

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

Положення розроблене з урахуванням вимог законів України «Про 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 Положення 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;

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.

II 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 **109**: 47 – персональні, 47 – портативні, 15 – планшети. (з них в робочому стані – 14, не працюють – 1) (з них в робочому стані 108, не працюють -1) *(відповідно до показника рядка 01 (2 розділу XIII); працюючих – XXX (із показника рядка 01 (2 розділу XIII) віднімаємо показник ЗНЗ-1 у рядках 03. Розділу XII).*

2. Із загальної кількості персональних комп'ютерів (в робочому стані) - **108**:
- робочі місця з комп'ютером у кабінеті основ інформатики й обчислювальної техніки для практичних занять з інформатики складає **13** *(відповідає показнику ЗНЗ-1 рядок 19 (6 розділу XII);*

- портативних комп'ютерів - **12** *(відповідає показнику ЗНЗ-1 у рядках 16-20. Розділу XII);*

- планшетів - **0** *(відповідає показнику ЗНЗ-1 у рядках 17. Розділу XII).*

3. В користуванні адміністрації – **6** персональних комп'ютерів, **0** стаціонарних комп'ютерів, **5** – портативних комп'ютерів, **0** – планшети.

4. В користуванні педагогічних працівників – **27** персональних комп'ютерів, із них **0** – стаціонарних, **27** – портативних *(загальна кількість працюючих персональних комп'ютерів віднімаємо кількість робочих місць з комп'ютером у кабінеті основ інформатики й обчислювальної техніки), що складає 26 % (відсотків від загальної кількості працюючих комп'ютерів).*

5. В користуванні адміністрації – всього **11** персональних комп'ютерів що складає 10 % (відсотків від загальної кількості працюючих комп'ютерів в ЗО), із них **6** - персональних комп'ютерів, 0 – стаціонарних комп'ютерів, 5 – портативних, 0 – планшетів.

6. Наявність комп'ютерної техніки, якій більше 5 років, складає: 33 (відповідає показнику 04 розділу XIII Звіту ЗНЗ – 1).

7. Кількість персональних комп'ютерів версії операційних систем – Windows (7,10,11) – 7, 10 або Linux складає: 0 (відповідає показнику рядків 10, 11, 12 розділу XIII звіту ЗНЗ – 1).

Налаштування та обслуговування комп'ютерів працівників

Загальні настанови та рекомендації щодо налаштувань і доступів до мережі:

1. Пароль і безпека:

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

Регулярно оновлюйте паролі і уникайте використання слабких або очевидних паролів.

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

2. Оновлення програмного забезпечення:

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

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

Захист від шкідливих програм.

3. Встановіть надійне антивірусне програмне забезпечення та антивірусні програми.

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

Уникайте відкриття підозрілих посилань або вкладень в електронних листах.

4. Налаштування мережі:

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

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

5. Налаштування файрволу:

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

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

6. Керування обліковими записами:

Створюйте окремі користувачів для кожного працівника та надавайте їм відповіді.

Ліцензійне програмне забезпечення

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

У закладі використовується наступне програмне забезпечення:

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.

перелік програмного забезпечення, що використовується у ЗЗСО згідно з типом ліцензії.

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, заступнику директора з АГЧ або уповноваженій особі.

4. Інженер-електронік (за його відсутності - уповноважена особа) має оглянути пристрої, якими користувався працівник, що звільняється, впевнитись в їх справності/скласти акт про несправність та повідомити керівництво закладу.

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

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

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

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, ПІН, 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.

Обслуговування комп'ютерів, які використовуються для спільної роботи (учнівські комп'ютери, комп'ютери у читальному залі бібліотеки, у медіатеці, в учительській 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 шкільної мережі Wi-Fi.
3. Налаштувати сканер безпеки на ПК. Налаштовувати брандмауер (фаєрвол): виявляє та блокує мережевий трафік на основі попередньо визначених або динамічних правил.
4. Слідкувати за оновленнями: переконатися, що отримуються автоматичні оновлення від служби Windows Update і інсталивати всі необхідні для організації оновлення.
5. Заборонити інсталивати програмне забезпечення з-поза меж організації, яке не затверджено або не адмініструється у закладі.
6. Безпечно зберігати дані. Заклад надає ресурс для зберігання даних, як-от GoogleDrive або інше корпоративне сховище. Не зберігати дані лише на локальному комп'ютері.
7. Постійно нагадувати (створювати пам'ятки, викладати їх на видне місце) щодо правил безпеки.

III. Налаштувати наступні рівні захисту:

- 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);

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 SUBNET, SIPCOM, який забезпечує доступ до Інтернету через кабель (*DSL, оптичний 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	
Інтернет провайдер закладу освіти	1
Тип підключення закладу освіти до мережі Інтернету (бездротовий Wi-Fi або провідний Ethernet)	2
Налаштування доступу до мережі Інтернету закладу освіти шляхом введення облікових даних, таких як ім'я користувача та пароль	Так

В закладі освіти не встановлені засоби відеоспостереження.

III РОЗДІЛ. Електронне діловодство закладу освіти

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

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

Ведення та зберігання ділової документації закладу освіти в електронній формі, спільна робота з електронними документами, обмін інформацією, як усередині організації, так і в зовнішній її комунікації, здійснюється із застосуванням одного з хмарних рішень для роботи з документами *Google Drive* на корпоративній платформі *Google*.

Власником файлів, які зберігаються в хмарному середовищі закладу освіти, є директор закладу освіти – Бобруль Т.О.

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 деяких з них – керівники шкільних методичних об'єднань.

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 (секретар – діловод – Чаглій Вікторія Іванівна) 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. Проекти 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.

Окремо, на порталі «NZ.UA» зберігаються документи з визначеним доступом та обмеженнями:

1. електронний журнал (адміністрація, вчителі – редагування);
2. електронний щоденник (батьки, учні – перегляд, комунікація);
3. таблиці успішності (класні керівники – редагування, батьки, учні - перегляд);
4. журнал реєстрації інструктажів (адміністрація – редагування, класні керівники - перегляд);
5. журнал замін, протоколи педради (адміністрація – редагування);
6. особова справа учня (адміністрація, класний керівник – редагування);
7. алфавітна книга запису учнів (офісний службовець (редагування, друк).

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

Доступ до щоденника учням і батькам надається класними керівниками.

До персональних даних в системі ІСУО мають доступ директор, заступники директора, з обмеженнями – класні керівники та вчителі закладу.

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

Інформація, яка обробляється в «КУРС: Школа», 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 учнів (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.

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

Сайт розміщено на українському сервері - <https://www.znvk41.school.social/> Конкретні хостинг-провайдер і доменне ім'я затверджуються наказом керівника закладу освіти.

Сайт закладу освіти не розміщується на серверах в країнах або належних компаніям та громадянам країн (у тому числі й афілійованих з ними), з якими в Україні 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 звільненні адміністратора/редактора сайту впродовж доби здійснюється зміна паролів.

При звільненні 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, учнів, може бути розміщена на окремих блогах та сайтах, спеціалізованих сайтах, доступ до яких організовується із сайту закладу.

Забороняється розміщення на сайті закладу освіти інформації рекламного 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:

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

Заклад освіти забезпечує механізм, щоб здобувачі освіти та/або їхні батьки, або особи, які їх замінюють, мали безстрокове право скасувати свою згоду на обробку особистих даних, вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання 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.

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 учнів/вихованців до закладу освіти, кількість вільних місць тощо*).

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

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

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

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

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

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

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

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

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

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

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

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

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: zschoool41@ukr.net (адреса)

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

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 вчителів, адміністрації та учнів).

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, Telegram. .

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)».

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 та 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 спілкування вчителів та учнів класу чи паралелі; для обміну інформацією між вчителем та батьками класу та інші.

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.

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

Загальні правила щодо спілкування в чатах обговорюються на засіданнях колегіального органу управління закладом освіти (педради), органів самоврядування (зокрема, учнівського, батьківського), додаються до правил поведінки (внутрішнього розпорядку), прийнятих в закладі освіти.

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

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

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

– *Не поширюйте неперевірену інформацію.*

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

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

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

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

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

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

Правила закріплюються у чаті за допомогою відповідної функції закріплення повідомлень.

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

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

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

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

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

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

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, Нові знання.

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.

Створено електронні журнали на платформі Нові знання.

Надано доступ для перегляду та редагування змісту відповідних сторінок електронного журналу членам адміністрації, класним керівникам, вчителям; для перегляду (теми уроку, домашні завдання, результати навчальних

досягнень учнів) – учням та батькам. Визначено відповідальну особу за координацію роботи персоналу з електронним журналом.

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

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

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 вчителями та учнями під час дистанційного навчання особистих домашніх пристроїв, які зазвичай не охоплюються мережним захистом, проводиться робота щодо ознайомлення вчителів та батьків учнів 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; вивченню функціоналу програмних засобів, визначених для організації освітнього процесу (формування запрошення на відеоконференцію учнів класу, блокування чату, надання різного роду доступів: до демонстрації екрану, спільного використання онлайн-документів, онлайн-дошки під час відеоконференції тощо); надання рекомендацій учителям, батькам учнів 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 циклу (навчального року, семестру, чверті) вчителем на уроці проводиться обов'язкове ознайомлення учнів з переліком ресурсів, які використовуватимуться в навчанні, надаються інструкції до роботи з вказаними з цифровими інструментами.

З метою ознайомлення батьків учнів з інтерактивними технологіями, які використовуватимуться вчителем, створюються стислі пам'ятки щодо роботи в ресурсі або з цифровим інструментом, відеоінструкції тощо, які розміщуються в електронному журналі поряд з відповідним завданням (*на сайті закладу освіти, на сайті вчителя тощо*).

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.

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 тому числі на матеріальних носіях;

- забезпечення захисту інформаційних ресурсів закладу освіти;

- проведення, за потреби, відповідної профілактичної роботи з учнями.

Визначено відповідальну особу за розгляд інцидентів, пов'язаних з онлайн-безпекою, та організацію відповідної просвітницької роботи.

В закладі освіти прийнято правила (вимоги) проведення дистанційного (онлайн) заняття: визначені умови підключення до онлайн-уроку; правила поведінки на уроці; використання мікрофону та камери учнями; правила використання чату, спілкування в чаті під час онлайн-уроку; використання спільного доступу до онлайн-інструментів під час уроку; умови присутності батьків здобувачів освіти на онлайн-уроці; рекомендації до зовнішнього вигляду учасників освітнього процесу, застосування фонових зображень тощо. Правилами також визначається умови видалення, блокування учасників освітнього заходу в разі порушення ними цих правил та умови повторного приєднання до онлайн-заходу.

Такі правила обговорюються та приймаються колективно, вносяться до правил поведінки в закладі освіти (*визначаються Стратегією (Положенням) про дистанційне навчання в закладі освіти, окремо затверджуються наказом керівника закладу освіти, інші*).

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

Використання мобільних пристроїв в освітніх цілях під час очного навчання допомагає урізноманітнити уроки, сприяти навчанню учнів, зокрема розвивати в них медіаграмотність.

З метою запобігання порушень дисципліни під час навчального процесу (відволікання учнів від навчання при використанні мобільних пристроїв не за призначенням, допущення учнями академічній недоброчесності, зниження рівня міжособистісного спілкування, яке є важливим для розвитку учнів, сприяння булінгу, неправомірній фото- чи відеозйомці та злочинам як проти самої дитини,

так і з боку дитини тощо) в закладі освіти застосовується обмеження користування мобільним пристроєм.

Учню закладу освіти не забороняється брати з собою до закладу освіти мобільний телефон, планшет, інші девайси, гаджети за умови безпеки цих пристроїв, відсутності загрози для безпеки і життя учасників освітнього процесу.

Використання мобільного пристрою під час освітнього процесу дозволяється:

- під час уроку за прямим дорученням (дозволом) вчителя для виконання навчального завдання тривалістю не більше визначеного вчителем для виконання завдання часу (пошук інформації, сканування QR-коду для отримання доступу до навчального матеріалу, тесту тощо, робота з документами зі спільним доступом, робота над навчальним проектом тощо);

- для екстреного зв'язку з батьками, але у спеціально відведених для цього місцях у закладі або за певних умов

Використання мобільного гаджету (смартфону) не рекомендується:

- учням початкової школи впродовж перебування в закладі освіти (за виключенням виконання навчального завдання (за умови дотримання норм тривалості роботи з технічними засобами навчання), здійснення екстреного зв'язку з батьками);

- учням 5-7 класів під час перерви між навчальними заняттями (за виключенням здійснення екстреного зв'язку з батьками);

Використання мобільного гаджету забороняється:

- під час уроку без прямого дозволу вчителя на використання гаджету в чітко визначений час та умови використання;

- для здійснення фото- чи відео зйомки учнів, однокласників, вчителів без їхньої згоди (може вважатися втручанням у приватне життя);

- для розповсюдження фотографій або повідомлень, які містять залякування чи переслідування (може призвести до кримінальної відповідальності).

В разі прямого порушення учнем заборони, висловленої вчителем щодо використання пристрою під час навчального заняття, питання щодо порушення дисципліни може розглядатись під час засідання Ради профілактики правопорушень закладу освіти (за участю батьків здобувача освіти).

Умови та правила використання мобільних технологій та інших електронних пристроїв в закладі освіти обговорюються та приймаються колективно, вносяться до правил поведінки в закладі освіти (*окремо затверджуються наказом керівника закладу освіти, інші*).

Про дотримання цих правил інформуються всі учасники освітнього процесу.

VIII РОЗДІЛ. Проведення заходів просвітницького характеру

З метою дотримання права дитини на безпеку та захист, яке є базовим та поширюється на її життєдіяльність як онлайн, так і офлайн, з урахуванням пріоритетного значення цифрових компетентностей для ефективного навчання та успішного життя людини в сучасному світі, формування навичок безпечної

поведінки дитини в цифровому середовищі з раннього віку в закладі освіти проводиться система профілактичних заходів просвітницького характеру з підвищення рівня знань в області інформаційно-комунікативних технологій, з питань безпечної поведінки в інтернеті, медіаграмотності.

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

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

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

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

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

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, бути складовою даного Положення, додатком до річного плану роботи закладу освіти, інш).*

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

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

Проведення заходів відповідно до Програми просвітницької роботи може здійснюватись відповідальною особою, призначеною керівником закладу освіти (наприклад, соціальним педагогом), класним керівником під час проведення тематичних класних годин, батьківських зборів, вчителем інформатики під час навчальних занять.

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

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

Орієнтовна Програма просвітницької роботи з учасниками освітнього процесу.

I Просвітницькі заходи з учителями (вихователями) як суб'єктами гарантування цифрової безпеки.

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

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

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

Для забезпечення правильного формування цифрової компетентності педагога він повинен мати:

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

№ з/п	Просвітницькі заходи	Примітки
1.	Для підвищення рівня обізнаності освітян щодо небезпек в мережі Інтернет: організація семінарів та навчальних курсів для освітян з питань цифрової безпеки, які охоплюють теми захисту персональних даних, безпеки паролів, використання безпечних мереж Wi-Fi, виявлення фішингових атак та інші аспекти цифрової безпеки.	Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р

2.	Для здобуття освітянами цифрової освіти з використанням інформаційних ресурсів: підготовка та розповсюдження матеріалів: пам'яток, брошур або інші матеріали з цифровою безпекою, які освітяни можуть використовувати в своїй роботі з учнями та вихованцями; надання учителям та вихователям як суб'єктам гарантування цифрової безпеки доступу до актуальних інформаційних ресурсів та рекомендацій з цифрової безпеки.	Згідно з ключовими положеннями, передбаченими Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
3.	Для обміну досвідом освітян як суб'єктів гарантування цифрової безпеки: створення форуму або онлайн-спільноти, де працівники закладу освіти зможуть обмінюватися досвідом та кращими практиками з цифрової безпеки; ділитися успішними стратегіями використання цифрових інструментів в професійній діяльності.	
4	Для підвищення рівня медіакультури та медіаграмотності: проведення тренінгів та майстер-класів для освітян з використанням сучасних інструментів для створення пізнавальних ігор та інтерактивних ресурсів; створення/перегляд/обговорення методики використання спеціальних мультиплікаційних відеороликів, які наголошують на безпеці в Інтернеті для дошкільнят та молодших школярів; встановлення партнерства з місцевими медійними організаціями або журналістами для проведення майстер-класів, тренінгів або стажування для учнів, де вони зможуть поглибити свої знання з медіа грамотності.	Згідно з реалізацією напрямів Стратегії інформаційної безпеки на період до 2025 року, затверджена указом Президента України від 28.12.2021 №685/2021
5	Для підвищення рівня інфомедійної культури педагогів в соціальних мережах: сприяння участі педагогів у вебінарах, прослуховуванні навчальних курсів, тренінгах, інтерактивних формах навчання, які формують складові інфомедійної культури дорослого особисто та як тренера для дітей у подальшому.	

6	Для підвищення практичних вмінь педагогів щодо побудови партнерських взаємовідносин між закладом освіти і родиною з питань безпечної поведінки дитини у цифровому середовищі: проведення тренінгів для формування навичок комунікації з батьками з питань поведінки у цифровому просторі; формування навичок стимулювання у батьків соціальної активності щодо обміну досвідом з питань формування безпечної поведінки дітей у цифровому просторі.	МОНУ (№1/9-128 від 10.03.2021 «Щодо необхідності проведення додаткових профілактичних заходів в середовищі дітей та підвищення обізнаності батьків»).
---	---	--

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

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

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

- не розповсюджує особисті дані (адресу проживання, місце навчання, номер мобільного телефону, інформацію про батьків) в Інтернеті;
- якщо трапилась неприємна ситуація – звертається по допомогу до дорослих, кому дитина довіряє (батьки, старший брат чи старша сестра, вихователь у садочку);
- не зустрічається (не прагне зустрітись) з тими, кого ми знаємо тільки онлайн;
- не відповідає на повідомлення, які є неприємними, повідомляє про них дорослому;
- розповідає (готовий розповісти) батькам, якщо хтось надсилає чи говорить неприємні слова;
- ні з ким не ділиться (знає правило) своїм паролем до гаджету чи додатку, доступом до власного профілю в соцмережі тощо;
- перед завантаженням нового додатку запитує (запитає) дозволу у батьків (діти 4-6(7) років).

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

3. До заходів просвітницького характеру з учасниками освітнього процесу (учні, вихованці) щодо попередження інформаційної небезпеки включаються

заходи щодо медіа грамотності, формування культури кібербезпеки та інфомедійної культури у цілому.

№ з/п	Просвітницькі заходи	Примітки
1.	Для підвищення свідомості учнів та вихованців щодо кібербулінгу: організація лекцій та презентацій з теми кібербулінгу, щоб ознайомити учнів з основними поняттями, причинами та наслідками цього явища; проведення виховних годин на тему важливості поваги до інших людей в онлайн-середовищі та спільного створення позитивного і безпечного інтернет-середовища; організація групових дискусій, де учні зможуть ділитися своїм досвідом та думками щодо кібербулінгу; розробка та проведення тематичних рольових ігор, де учні (вихованці) зможуть імітувати ситуації кібербулінгу та навчатися реагувати на них.	Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
2.	Для навчання правилам безпечної поведінки учнів (вихованців) в Інтернеті: організація розважальних активностей, які сприяють розвитку безпечної поведінки в Інтернеті для дітей старшого дошкільного та молодшого шкільного 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; відвідування експертів з безпеки в Інтернеті або представників поліції, які спеціалізуються на кібербезпеці, для	Вікова категорія до 12 років Згідно з реалізацією напрямів Стратегії інформаційної безпеки на період до 2025 року, затверджена указом Президента України від 28.12.2021 №685/2021 Згідно з напрямами Стратегії кібербезпеки України, затвердженої указом

	проведення презентацій, лекцій, зустрічей, для надання корисних порад учням (вихованцям); проведення практичних воркшопів та тренінгів на теми сильних паролей, розпізнавання фішингових атак, контроль приватності та безпека соціальних мереж, де учні зможуть навчатися практичним навичкам безпеки в Інтернеті; створення та проведення інтерактивних ігор та квіз-конкурсів на тему кібербезпеки, де учні зможуть вирішувати завдання, пов'язані з безпекою в Інтернеті; організація екскурсій для учнів до місцевих центрів кібербезпеки або інших організацій, що займаються безпекою в Інтернеті для ознайомлення з місцем роботи експертів та заходами, які приймаються для захисту від кіберзагроз.	Президента України від 26.08.2021 №447/2021
2.1	Теми для заходів щодо попередження інформаційної безпеки: 1. Основи кібербезпеки: навчання учасників освітнього процесу про загрози, які можуть виникнути в інтернеті, і про те, як захистити свої особисті дані та пристрої. 2. Соціальна інженерія: навчання про те, як кіберзлочинці можуть використовувати соціальні мережі та електронну пошту для отримання доступу до особистих даних та фінансових ресурсів. 3. Віруси та шкідливі програми: навчання про те, як віруси та шкідливі програми можуть поширюватися через повідомлення електронної пошти або за допомогою миттєвих повідомлень.	Вікова категорія 12-15 років

3.	Для підвищення рівня медіакультури та медіаграмотності: організація бесід та презентацій про джерела інформацій, фейкові новини, рекламу та вплив медіа на наше сприйняття світу; проведення дебатів та обговорень з учнями про вплив соціальних медіа, роль реклами у формуванні думок, етичні питання та обмеження медіа; запрошення медіаекспертів або представників організацій, що займаються медіаграмотністю для проведення виступів або дискусій та ознайомленням з роботою в цій сфері; проведення практичних ворк-шопів, де учні матимуть можливість самостійно працювати з медіа, навчатися створювати власні медійні продукти з ефективним використанням медіа-інструментів; залучати учнів до критичного аналізу новин з метою розпізнавання фейкових новин, знаходження джерела інформації та перевірки достовірності фактів; розвиваємо вміння розрізняти об'єктивну інформацію від прихованої маніпуляції; проведення майстер-класів, тренінгів або стажування для учнів, де вони зможуть поглибити свої знання з медіаграмотності.	Вікова категорія 12-17 років Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
----	---	---

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

1. Проведення заходів щодо визначення ступеню розуміння батьками питання безпеки комунікації дитини у цифровому просторі.
2. Актуалізація визначення рівня довіреності відносин дітей та батьків.
3. Опитування батьків щодо засобів комунікації, якими користується дитина у цифровому просторі.
4. Плануванні заходів для батьків щодо попередження інформаційної небезпеки з урахуванням актуальних потреб учасників освітнього процесу.

Просвітницькі заходи	Зміст заходів						
1.	Батьки у цифровому суспільстві <table border="1" data-bbox="284 365 1552 1449"> <tr> <td data-bbox="284 365 561 797">1.1. Цифрове суспільство</td><td data-bbox="561 365 1552 797"> 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 </td></tr> <tr> <td data-bbox="284 797 561 1039">1.2. Електронне урядування</td><td data-bbox="561 797 1552 1039"> Використання цифрових технологій та сервісів для: – підтримки та участі у електронному урядуванні; – розуміння понять «відкриті дані», «електронна ідентифікація громадян», «цифрові державні платформи» тощо; </td></tr> <tr> <td data-bbox="284 1039 561 1449">1.3. Електронний заклад освіти</td><td data-bbox="561 1039 1552 1449"> Використання цифрових сервісів та технологій для: – створення «цифрового робочого місця» дитини; – розуміння цифрового освітнього середовища закладу (класу, групи); – заохочення батьків та громадськості до ефективного використання цифрового освітнього середовища закладу (групи); – активного сприяння використанню цифрових технологій для комунікації із закладом освіти. </td></tr> </table>	1.1. Цифрове суспільство	Використання цифрових технологій та сервісів для: – розуміння ролі цифрових ресурсів у житті громадянина та суспільства; – вирішення проблем та завдань у повсякденному житті, особистої взаємодії, спілкування, перегляду ресурсів, даних та відомостей; – участі у суспільній діяльності; – захисту своїх прав та свобод, вираження власної громадянської позиції	1.2. Електронне урядування	Використання цифрових технологій та сервісів для: – підтримки та участі у електронному урядуванні; – розуміння понять «відкриті дані», «електронна ідентифікація громадян», «цифрові державні платформи» тощо;	1.3. Електронний заклад освіти	Використання цифрових сервісів та технологій для: – створення «цифрового робочого місця» дитини; – розуміння цифрового освітнього середовища закладу (класу, групи); – заохочення батьків та громадськості до ефективного використання цифрового освітнього середовища закладу (групи); – активного сприяння використанню цифрових технологій для комунікації із закладом освіти.
1.1. Цифрове суспільство	Використання цифрових технологій та сервісів для: – розуміння ролі цифрових ресурсів у житті громадянина та суспільства; – вирішення проблем та завдань у повсякденному житті, особистої взаємодії, спілкування, перегляду ресурсів, даних та відомостей; – участі у суспільній діяльності; – захисту своїх прав та свобод, вираження власної громадянської позиції						
1.2. Електронне урядування	Використання цифрових технологій та сервісів для: – підтримки та участі у електронному урядуванні; – розуміння понять «відкриті дані», «електронна ідентифікація громадян», «цифрові державні платформи» тощо;						
1.3. Електронний заклад освіти	Використання цифрових сервісів та технологій для: – створення «цифрового робочого місця» дитини; – розуміння цифрового освітнього середовища закладу (класу, групи); – заохочення батьків та громадськості до ефективного використання цифрового освітнього середовища закладу (групи); – активного сприяння використанню цифрових технологій для комунікації із закладом освіти.						

Безпека в цифровому суспільстві	Використання цифрових сервісів та технологій для: – розпізнавання та протидії маніпуляційних технологій і пропаганди, перевірки надійності джерел і достовірності даних, небезпек в цифровому просторі; – розуміння важливості відповідальної і безпечної поведінки в цифровому просторі; – уникнення ризику здоров'я і загроз для фізичного і психологічного благополуччя при роботі у цифровому просторі; – запобігання онлайн-злочинів в цифровому суспільстві; – формування вміння захистити цифрові пристрої, дані та інші ресурси; – знання заходів безпеки, розуміння персональної відповідальності кожного щодо ризиків та загроз при використанні цифрових пристроїв і мереж; – захисту персональних даних та приватності; – захисту навколишнього середовища, тобто розуміння впливу цифрових технологій на навколишнє середовище, з точки зору їх утилізації, а також їх використання, що може нанести шкоду, наприклад, об'єктам критичної інфраструктури тощо
2. Розвиток цифрової компетентності батьків Використання цифрових сервісів для спілкування, співпраці батьків та закладу освіти	
2.1. Комунікація. Використання цифрових сервісів для покращення комунікації батьків із закладом освіти або третіми особами. Розвиток співпраці та вдосконалення організаційних стратегій комунікації	Використання цифрових сервісів для: – участь у онлайн-заходах для спілкування з закладом освіти, дотримання, наприклад, правил, зустрічі, заходів тощо; – отримання інформації (індивідуально або колективно) від закладу освіти, наприклад, про особистий прогрес дитини у навчанні та з проблемних питань, що викликають стурбованість; – спілкування з іншими батьками (різними педагогами) в 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: - формувати 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 цифровій компетентності щодо налаштування цифрових пристроїв і сервісів; - підтримки інших в розвитку їх цифровій 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 гаджетів та цифрового середовища та підвищувати самооцінку дитини, дозволяти дитині самостійно робити вибір і бути відповідальною за це;
- заохочувати користуватися гаджетами в зонах видимості дорослих;
- встановлювати часові межі користування гаджетами 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).

З метою визначення потреби, змісту та напрямків просвітницької роботи з учасниками освітнього процесу в закладі освіти проводиться відповідний моніторинг, на підставі результатів якого формується план заходів на наступний навчальний рік.

Питання щодо організації просвітницької роботи в закладі освіти щодо формування/удосконалення цифрових навичок учасників освітнього процесу є предметом розгляду на засіданнях методичних об'єднань вчителів, педагогічної ради.

ІХ 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.

Х РОЗДІЛ. Прикінцеві положення

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

Порядок обговорення оновлень визначається педагогічною радою.

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

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

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

Використані джерела:

РОЗДІЛ	Використані джерела
II	https://zakon.rada.gov.ua/laws/show/z0582-18#n13 https://zakon.rada.gov.ua/laws/show/3792-12#Text https://zakon.rada.gov.ua/laws/show/z0044-05#Text https://uk.wikipedia.org https://ips.ligazakon.net/document/view/KR020247?an=88
III	Курс “Цифрова безпека для громадських організацій в умовах війни” від “Prometheus” https://naurok.com.ua/post/dilova-dokumentaciya-zakladu-osviti-stvorenniya-dokumentiv-v-elektronniy-formi - Закон України №2297-VI «Про захист персональних даних». - Наказ МОН України від 08.08.2022 № 707 “Про затвердження Інструкції з ведення ділової документації у закладах загальної середньої освіти в електронній формі” - Наказ МОН України від 25.06.2018 № 676 “Про затвердження Інструкції з діловодства у закладах загальної середньої освіти”
IV	https://naurok.com.ua/polozhennya-pro-sayt-zakladu-osviti-283304.html
VII	https://mon.gov.ua/storage/app/media/zagalna%20serednya/metodichni%20recomendazii/2020/metodichni%20recomendazii-dustanciyna%20osvita-2020.pdf https://www.helsinki.org.ua/articles/orhanizatsiia-dystantsiynoi-formy-osvity-v-zzso-v-umovakh-voiennoho-stanu-na-shcho-potribno-zvernuty-uvahu/ https://jurfem.com.ua/bezpechna-shkola-vyklyky-systemy-osvity-v-umovakh-viyny/ https://osvita.ua/school/79806/ https://sqe.gov.ua/yak-vchitelyu-organizuvati-svoyu-robotu-p/
VIII	https://docs.google.com/document/d/1iQsUdO0NeURqX907RGALd9KMFjSqYcKK/edit?usp=sharing&oid=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/