

СХВАЛЕНО

на засіданні педагогічної ради
Центральноукраїнського
наукового ліцею Кіровоградської
обласної ради
Протокол № 5 від 30.05.2025

ЗАТВЕРДЖУЮ

наказ Центральноукраїнського
наукового ліцею Кіровоградської
обласної ради
Директор
Неля МАЗУР
від _____ № _____

**ПОЛОЖЕННЯ
ПРО ЦИФРОВУ БЕЗПЕКУ
Центральноукраїнського наукового ліцею
Кіровоградської обласної ради**

ЗМІСТ

I РОЗДІЛ. Загальні положення.....	3
II РОЗДІЛ. Технічне забезпечення цифрового освітнього простору	5
2.1. Забезпеченість робочими комп'ютерами	5
2.2. Налаштування та обслуговування комп'ютерів працівників	5
2.3. Ліцензійне програмне забезпечення	7
2.4. Порядок оновлення доступу при звільненні працівника	8
2.5. Збереження інформації.....	8
2.6. Робота з паролями	9
2.7. Обслуговування комп'ютерів, які використовуються для спільної роботи здійснюється уповноваженою відповідальною особою.....	9
2.8. Функціонування підключення до мережі інтернет	10
III РОЗДІЛ. Електронне діловодство	10
IV РОЗДІЛ. Сайт закладу освіти	12
V РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти (електронна пошта)	15
VI РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти	16
VII РОЗДІЛ. Особливості організації цифрової безпеки освітнього процесу. .	18
7.1. Цифрові інструменти реалізовані засобами освітньої інформаційної системи «Мрія».....	18
7.2. В закладі освіти визначено порядок реагування працівників на інциденти, пов'язані з безпекою дітей	18
7.3. В закладі освіти визначено порядок проведення дистанційних (онлайн) занять у разі надзвичайних ситуацій.....	19
7.4. В закладі освіти встановлюються умови та правила використання мобільних технологій та інших електронних пристроїв під час навчальних занять.	19
VIII РОЗДІЛ. Проведення заходів просвітницького характеру	20
8.1. Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки з педагогічними працівниками:	22
8.2. Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки з учнями (вихованцями):	23
8.3. Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки з батьками (іншими дорослими, які опікуються вихованням дитини):	26
IX РОЗДІЛ. Захист персональних даних в цифровому середовищі закладу освіти	27
X РОЗДІЛ. Прикінцеві положення	28

ПОЛОЖЕННЯ

Про цифрову безпеку Центральноукраїнського наукового ліцею Кіровоградської обласної ради

І РОЗДІЛ. Загальні положення

Положення «Про цифрову безпеку закладу освіти» визначає політику цифрової безпеки Центральноукраїнського наукового ліцею Кіровоградської обласної ради (далі – ЛІЦЕЙ).

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. Технічне забезпечення цифрового освітнього простору

Цифровий освітній простір ЛІЦЕЮ складають наступні компоненти:

- **внутрішні:** комп'ютери, засоби відеоспостереження, цифрове діловодство, освітня інформаційна система;
- **зовнішні:** вебсайт закладу освіти, блоги працівників, месенджери, соціальні мережі, освітня інформаційна система.

2.1. Забезпеченість робочими комп'ютерами

1. Загальна кількість персональних комп'ютерів в закладі освіти складає 206 (з них в робочому стані - 44 не працюють - 6)
2. Із загальної кількості персональних комп'ютерів (в робочому стані) - 194:
3. робочі місця з комп'ютером та/або ноутбуком у кабінеті основ інформатики й обчислювальної техніки для практичних занять з інформатики складає 60;
4. портативних комп'ютерів – 36;
5. планшетів - 15.
6. У користуванні адміністративно-господарської частини – 53 комп'ютерів (з них 53 стаціонарних комп'ютерів, що складає 27% від загальної кількості працюючих комп'ютерів).
7. У користуванні педагогічних працівників – 23 персональних комп'ютерів, із них 23 – стаціонарних, що складає 12 % від загальної кількості працюючих комп'ютерів.
8. Наявність комп'ютерної техніки, якій більше 5 років, складає 175 од.
9. Кількість персональних комп'ютерів версії операційних систем – Windows (7,10,11) – 192 шт. та Linux – 2 шт.

2.2. Налаштування та обслуговування комп'ютерів працівників

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

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

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

Відповідальна особа закладу освіти надає настанови та рекомендації щодо необхідних налаштувань та доступів до мережі, але виконання цих налаштувань є зоною відповідальності працівників (у закладі функціонує мережева система, працівники і учні, акаунти яких шифруються паролями).

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 закладу освіти		ПІБ відповідальної особи
Адміністратор мережі (інженер електронік, відповідальна особа)		ПЄНІНА Альона Олегівна (за відсутності відповідальна особа – ВЕЛИКОІВАНЕНКО Сергій Вадимович, МИРОНЕНКО Віктор Анатолійович)
Уповноважені особи	Особа, відповідальна за ведення шкільної сторінки Facebook	ДЕНИСОВ Денис Олександрович
	Особа, відповідальна за підтримку та налаштування освітньої інформаційної системи закладу, надання електронної статистичної звітності, замовлення підручників	ВЕЛИКОІВАНЕНКО Сергій Вадимович
	Особа, відповідальна за функціонування шкільного сайту, його налаштування	ПЄНІНА Альона Олегівна
	Особа, відповідальна ремонт та заправку оргтехніки	МИРОНЕНКО Віктор Анатолійович
Самостійне налаштування при роботі працівника на особистому комп'ютері. Обов'язкове ознайомлення працівників з «Загальними настановами та рекомендаціями щодо налаштувань і доступів до мережі»		

Загальні настанови та рекомендації щодо налаштувань і доступів до мережі:

1. Пароль і безпека:

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

Регулярно оновлюйте паролі і уникайте використання слабких або очевидних паролів.

Використовуйте двоетапну аутентифікацію, якщо це можливо, для додаткового

рівня безпеки.

2. Оновлення програмного забезпечення:

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

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

Увімкніть 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 та меседжерах.

4. Налаштування мережі:

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

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

5. 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 відповідні сильні паролі.

2.3. 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 (назви програм не розкриваються у зв'язку з можливими кібератаками):

1) З комерційною ліцензією – передбачає, що користувач оплачує вартість використання даної програми на одному чи кількох зазначених 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.

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

в. корпоративна ліцензія – ліцензія на кілька копій програми для використання.

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, при цьому можуть бути присутні платні послуги.

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.

2.4. 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 ГР.

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.

2.5. Збереження інформації

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

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

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

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

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

2.6. Робота з пароллями

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, ППН, 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;
- паролльні фрази;
- резервне копіювання для кожного способу.

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

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

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

1. Налаштувати захист. Доступ до груп налаштувати через корпоративні акаунти з будь-яких пристроїв.
2. Забезпечити коректне використання шкільної 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 інсталиувати всі необхідні для організації оновлення.
7. Заборонити інсталиувати 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 GoogleDrive 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.

2.8. Функціонування підключення до мережі інтернет

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

Доступ до мережі Інтернет здійснюється з резервуванням підключення до двох різних провайдерів Sila та Shtorm

Інтернет провайдери ЛПЦЕЮ	Sila, Shtorm
Тип підключення закладу освіти до мережі Інтернету (бездротовий Wi-Fi або провідний Ethernet)	Оптичне волокно
Налаштування доступу до мережі Інтернету закладу освіти шляхом введення облікових даних, таких як ім'я користувача та пароль	Наявне
Адміністратор мережі закладу освіти	ПЄНІНА Альона Олегівна ДЕНИСОВ Денис Олександрович

В закладі освіти встановлені засоби відеоспостереження (перший поверх, парадний вхід та подвір'я). Для забезпечення відео спостереження використовується обладнання: камери відеоспостереження, відеореєстратор.

Запис відео реєстратора зберігається на жорсткому диску.

III РОЗДІЛ. Електронне діловодство

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 внутрішньої системи захищених відкритих папок.

Для забезпечення роботи з електронними документами та своєчасного їх виконання у закладі освіти існує схема 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 (секретарем) вхідних листів через електронну пошту закладу освіти, реєстрація у відповідному електронному журналі вхідної документації, пересилання відповідному працівнику по утвердженому каналу (email або меседжер).

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

3. Контроль за виконанням резолюції здійснює діловод (секретар).

4. Проекти наказів, вихідних документів реєструються відповідальним за діловодство (секретарем) у відповідному журналі реєстрації наказів/вихідних документів. Доступ до електронних версій наказів, вихідних документів надається членам адміністрації відповідно до повноважень.

5. 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.

Окремо, на порталі «Мрія» зберігаються документи з визначеним доступом та обмеженнями:

1. електронний журнал;
2. електронний щоденник;
3. таблиці успішності;
4. журнал реєстрації інструктажів;
5. журнал замін, протоколи педради;
6. особова справа учня;
7. алфавітна книга запису учнів.

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

Доступ до щоденника учням і батькам надається класними керівниками. До персональних даних в системі «Мрія» 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.

Сайт створюється з метою спрощення комунікації всіх учасників освітнього процесу; інформування громадськості про особливості закладу освіти, історії його розвитку, про освітні програми та проекти 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.

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 власному сервері.

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

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

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

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

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

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

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

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

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

Відповідно до Закону України «Про засади запобігання та протидії

дискримінації в Україні» на сайті закладу освіти повинні бути відсутні вияви дискримінації, щодо віку, раси, кольору, статі, мови, релігії, політичних або інших переконань учасників освітнього процесу, національного, етнічного або соціального походження, майна, інвалідності, народження або іншого статусу.

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

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

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

Забороняється розміщення на сайті закладу освіти інформації 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:

Технічний захист - це аспект безпеки, що стосується 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 стосується 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, 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.

Сайт має містити підтвердження права третіх осіб на вільне поширення, використання та переробку інформаційних матеріалів у вигляді повідомлення:

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 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.

З урахуванням обмежень, визначених у стратегії розвитку закладу,

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

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)

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: ospa2005@ukr.net

VI РОЗДІЛ. Засоби зовнішньої комунікації закладу освіти

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, в класних групах в месенджерах та на офіційному сайті.

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 акаунта, зокрема, не зазначається геолокація (місце розташування освітнього закладу); здійснюється періодичний перегляд списку «друзів» у соціальній мережі (якщо серед них є незнайомі або підозрілі акаунти, необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу); не використовуються соціальні мережі та пошукові системи (у т.ч. із застосуванням сервісів VPN), доступ до яких обмежено відповідно до Указу Президента України «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

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

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

В закладі освіти таким засобом комунікації виступають захищені чати в середовищі «Мрія» та Telegram.

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.

Презентація закладу освіти в соцмережах, здійснення спілкування його працівників в месенджерах має бути коректним, професійним, етичним. Важливо сформулювати 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. Спілкування між співробітниками закладу освіти та учнями/вихованцями та/або батьками в закладі освіти здійснюється виключно до 20.00.

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 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 цифрової безпеки 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, технічних, кадрових можливостей, стратегічних перспектив розвитку закладу освіти.

Забезпечення цифрової безпеки необхідно в умовах сучасного організації освітнього процесу.

7.1. Цифрові інструменти реалізовані засобами освітньої інформаційної системи «Мрія».

Система дозволяє надавати 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.

7.2. 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 онлайновою безпекою, та організацію відповідної просвітницької роботи.

7.3. В закладі освіти визначено порядок проведення дистанційних (онлайн) занять у разі надзвичайних ситуацій.

Заняття проводяться на платформі Zoom, посилання на приєднання до уроків розсилаються через месенджери. На дистанційному уроці:

- ✓ 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.

Про дотримання цих правил інформуються всі учасники освітнього процесу.

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

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.

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 офлайн, так і онлайн, з урахуванням пріоритетного значення цифрових компетентностей для ефективного навчання та успішного життя людини в сучасному світі, формування навичок безпечної поведінки дитини в цифровому середовищі з раннього віку в закладі освіти проводиться система профілактичних заходів просвітницького характеру з підвищення рівня знань в області інформаційно-комунікативних технологій, з питань безпечної поведінки в інтернеті, медіаграмотності.

Для організації роботи з учасниками освітнього процесу в закладі освіти

здійснюються наступні кроки:

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.

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.

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

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.

Керівник закладу призначає відповідальну особу (осіб) з питання щодо просвіти учасників освітнього процесу.

Відповідальна особа на підставі попередньо проведеного моніторингу (опитування учасників освітнього процесу), з урахуванням особливостей організації освітнього процесу визначає напрямки просвітницької роботи: безпека користування пристроями, інтернетом.

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

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

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

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.

8.1. Заходи просвітницького характеру з учасниками освітнього процесу щодо попередження інформаційної небезпеки з педагогічними працівниками:

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 для педагогічних працівників	Примітки
1.	Проведення семінарів і тренінгів, де вчителі дізнаються, як захищати свої особисті дані, створювати надійні паролі, безпечно користуватися Wi-Fi, розпізнавати шахрайські листи (фішинг) та дбати про свою цифрову безпеку загалом.	Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р

2.	Проведення тренінгів і майстер-класів для вчителів, де вони навчатимуться використовувати сучасні інструменти для створення ігор та інтерактивних матеріалів. Також – перегляд і обговорення мультфільмів про інтернет-безпеку для дошкільнят та молодших школярів з акцентом на їх педагогічне використання. Запрошення місцевих журналістів чи представників медіа для співпраці – проведення майстер-класів, тренінгів або навіть стажування для учнів, щоб ті краще розуміли, як працюють медіа. Підвищення інфомедійної культури педагогів у соцмережах: заохочення вчителів до участі у вебінарах, тренінгах, онлайн-курсах та інших інтерактивних формах навчання. Це допоможе їм не лише вдосконалити власну інфомедійну культуру, а й навчати цього дітей.	Згідно з реалізацією напрямів Стратегії інформаційної безпеки на період до 2025 року, затверджена указом Президента України від 28.12.2021 №685/2021
3.	Проведення тренінгів, які допоможуть педагогам краще спілкуватися з батьками щодо безпечної поведінки дітей в інтернеті. Навчання вчителів, як залучати батьків до обміну досвідом і спільного обговорення способів захисту дітей у цифровому середовищі.	Згідно з листом МОН України №1/9-128 від 10.03.2021 «Про необхідність проведення додаткових профілактичних заходів у дитячому середовищі та підвищення обізнаності батьків»

8.2. 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 з учнями (вихованцями)	Примітки
1.	Проведення лекцій і презентацій, щоб учні зрозуміли, що таке кібербулінг, чому він виникає і які може мати наслідки. Під час виховних годин – розмови про повагу до інших у мережі та важливість створення дружнього й безпечного онлайн-середовища. Організація групових обговорень, де учні можуть поділитися власним досвідом або поглядами щодо кібербулінгу. Проведення рольових ігор – відтворення ситуацій кібербулінгу.	Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р
2.	Навчання учнів безпечній поведінці в Інтернеті: • Проведення веселих і пізнавальних активностей для дошкільнят та учнів початкової школи, які вчать безпечній поведінці онлайн. • Використання інтерактивних ігор для закріплення правил інтернет-безпеки. • Розміщення пам'яток і яскравих плакатів із правилами безпечної	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 Президента

	поведінки у школах і дитсадках — щоб діти могли легко запам'ятати головне. • Зустрічі з фахівцями з кібербезпеки або представниками поліції — вони проводять лекції, презентації та дають корисні поради дітям. • Організація практичних тренінгів і воркшопів для учнів, де вони навчаються створювати надійні паролі, розпізнавати фішинг, налаштовувати приватність у соцмережах. • Проведення ігор-квізів на тему інтернет-безпеки, де учні виконують завдання та перевіряють свої знання. • Екскурсії до центрів кібербезпеки або установ, які захищають людей в онлайн-просторі — щоб діти побачили, як працюють справжні експерти.	Українівід 26 08.2021 №447/2021
3.	Теми для заходів з інформаційної безпеки: 1. Як себе захистити в Інтернеті? – Що таке особисті дані і чому їх треба берегти? – Як не стати жертвою шахраїв? 2. Обережно: обман в соцмережах та листах – Як зловмисники змушують нас "віддати" свої дані – Як розпізнати підозрілі повідомлення 3. Віруси: як захистити свій комп'ютер – Що таке віруси і як вони потрапляють на пристрої – Чому не варто натискати на "подарунки" в інтернеті	Вікова категорія 12-15 років
4.	Заходи для підвищення медіакультури та медіаграмотності учнів: 1. Бесіди та презентації 2. Дебати та обговорення 3. Зустрічі з медіаекспертами 4. Практичні воркшопи 5. Навчання критичному мисленню 6. Майстер-класи, тренінги, стажування	Вікова категорія 12-17 років Згідно з Концепцією розвитку цифрових компетентностей, схваленою розпорядженням Кабінету Міністрів України від 03.03.2021 №167-р

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

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

№ з/п	Просвітницькі заходи з учнями (вихованцями)	Примітки
1.	Тема: У повсякденному житті - Обговорення: “Як Інтернет змінює наше життя” - Презентації про онлайн-сервіси, які допомагають у повсякденному житті	Формування розуміння користі цифрових технологій
2.	Тема: У взаємодії з державою. - Зустріч з фахівцем з “Дії” або працівником ЦНАПу - Перегляд відео або кейсів про електронні держпослуги	Формування цифрової грамотності громадянина
3.	Тема: Формування цифрової грамотності громадянина - Створення з учнями “ідеального цифрового робочого місця” - Практичне заняття: знайомство з електронним журналом, освітніми платформами	Навчання взаємодії учнів і батьків у цифровому середовищі
4.	Тема: Безпека у цифровому просторі. - Інтерактив: “Фейк чи правда?” - Тренінг: як перевіряти джерела і уникати маніпуляцій	Навчання безпечному та відповідальному використанню цифрових технологій
5.	Тема: Розвиток цифрової компетентності батьків - Батьківські збори онлайн: як працюють цифрові сервіси - Інструктаж: як переглядати успішність дитини через електронний щоденник	Залучення батьків до цифрового життя школи
6.	Тема: Використання цифрових ресурсів. - Огляд урок: “Які сайти ми можемо використовувати для навчання?” - Вправи: перевірка джерел на достовірність	Навчання вибору якісного й безпечного цифрового контенту

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.