

**СХВАЛЕНО**  
Протокол засідання педагогічної ради  
ЗНВК "Запорізька Січ"  
«19» вересня 2023 №4

**ЗАТВЕРДЖЕНО**  
Наказ ЗНВК «Запорізька Січ»  
«19» вересня 2023 №99/р

## **ПОЛОЖЕННЯ**

**Про цифрову безпеку**  
**Запорізького навчально-виховного комплексу «Запорізька Січ»**  
**військово-спортивного профілю**  
**Запорізької міської ради Запорізької області**

**м. Запоріжжя**  
**2023**

## I РОЗДІЛ. Загальні положення

Положення «Про цифрову безпеку Запорізького навчально-виховного комплексу «Запорізька Січ» військово-спортивного профілю Запорізької міської ради Запорізької області» визначає політику цифрової безпеки Запорізького навчально-виховного комплексу «Запорізька Січ» військово-спортивного профілю Запорізької міської ради Запорізької області (далі – ЗНВК «Запорізька Січ»).

Положення «Про цифрову безпеку Запорізького навчально-виховного комплексу «Запорізька Січ» військово-спортивного профілю Запорізької міської ради Запорізької області» (далі – Положення) описує основні принципи побудови системи управління інформаційною безпекою закладу освіти, посадових обов'язків і практик, які використовуються закладом освіти для зменшення цифрових ризиків та збереження персональних даних учасників освітнього процесу.

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

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

У Положенні нижченаведені терміни вживаються в такому значенні:

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

**безпека мережі** - здатність електронних комунікаційних мереж протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж, а також даних, що зберігаються, передаються чи обробляються;

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

**гаджет** – пристрій, пристосування, яке виконує обмежене коло завдань;

**дані** - інформація, яка подана у формі, придатній для її оброблення електронними засобами;

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

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

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

**засоби інформатизації** - комп'ютери, програмні продукти, інформаційні системи або їх окремі елементи, електронні комунікаційні мережі, що використовуються для реалізації інформаційно-комунікаційних технологій;

**захист інформації** - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

**інформатизація** - сукупність взаємопов'язаних організаційних, правових, технологічних, виробничих інших процесів, спрямованих на створення умов для забезпечення розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій;

**інформаційно-комунікаційні технології** - результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг;

**інформація** - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

**інформаційна діяльність** - це створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації;

**комунікація** - це процес спілкування і передачі інформації між людьми або їх групами у вигляді усних і письмових повідомлень;

**месенджер** – телекомунікаційна служба для обміну текстовими повідомленнями між комп'ютерами або іншими пристроями користувачів через комп'ютерні мережі;

**мобільний пристрій** – це загальний термін для будь-якого портативного комп'ютера або смартфон;

**оцифрування** - це створення цифрового зображення фізичних об'єктів або атрибутів; в рамках оцифрування не відбувається змін структури інформації, вона просто набуває електронну форму для подальшої обробки в цифровому форматі;

**персональні дані** - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

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

**соціальна мережа** – соціальна структура, утворена індивідами або організаціями, вебсайт або інша служба у Веб, яка дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок та переглядати власний список зв'язків і списки інших користувачів;

**хмарні технології** – це технології, які надають користувачам Інтернету доступ до комп'ютерних ресурсів сервера і використання програмного забезпечення як онлайн-сервіса;

**цифрова компетентність** – здатність використовувати цифрові медіа й електронні освітні ресурси (ЕОР), розуміти та критично оцінювати різні аспекти медіа - цифрових і контенту, а також якість, що вказує на рівень кваліфікації практичного використання ЕОР;

**цифрова технологія** - сукупність систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації;

**цифровізація** - процес впровадження цифрових технологій у всі сфери суспільного життя.

Інші терміни вживаються у даному Положенні у значеннях, визначених законодавчими актами України.

## **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, месенджери, соціальні мережі.

### **Забезпеченість робочими комп'ютерами**

1. Загальна кількість персональних комп'ютерів в закладі освіти складає 60 шт. (з них в робочому стані – 56 шт., не працюють – 4 шт.)

2. Із загальної кількості персональних комп'ютерів (в робочому стані) – 56 шт.:

- робочі місця з комп'ютером у кабінеті основ інформатики й обчислювальної техніки для практичних занять з інформатики складає 19 шт.;
- портативних комп'ютерів – 20 шт.;
- планшетів - 0.

3. В користуванні адміністрації – 12 шт. персональних комп'ютерів, з них 9 шт. стаціонарних комп'ютерів, 3 шт. – портативних комп'ютерів.

4. В користуванні педагогічних працівників – 37 шт. персональних комп'ютерів, із них 17 шт. – стаціонарних, 20 шт. – портативних.

5. В користуванні адміністрації – всього 12 шт. персональних комп'ютерів що складає 21%, із них 9 шт. – стаціонарних комп'ютерів, 3 шт. – портативних.

6. Наявність комп'ютерної техніки, якій більше 5 років, складає 27 шт.

7. Кількість персональних комп'ютерів версії операційних систем – Windows (7,10,11) або Linux складає 56 шт..

### **Налаштування та обслуговування комп'ютерів працівників**

Відповідно штатного розпису в ЗНВК «Запорізька Січ» є штатна посада інженер-електронік (1 ст.), який виконує налаштування комп'ютерів працівників, включаючи адміністратора мережі.

Інженер-електронік має 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.

Інженер-електронік закладу освіти надає настанови та рекомендації щодо необхідних налаштувань та доступів до мережі, але виконання цих налаштувань є зоною відповідальності працівників відповідно до «Загальних настанов та рекомендацій щодо налаштувань і доступів до мережі» (Додаток 1).

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

### **Ліцензійне програмне забезпечення**

На комп'ютерні програми, які використовуються в закладі освіти, поширюється дія Закону України «Про авторське право і суміжні права», і їх

використання можливе лише за умови дотримання вимог цього закону, а також вимог ліцензії, з якою користувач погоджується, установлюючи програму на свій комп'ютер.

У закладі освіти може використовуватися наступне програмне забезпечення:

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

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

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

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

Інженер-електронік створює перелік програмного забезпечення, що використовується у ЗЗСО згідно з типом ліцензій.

### **Порядок оновлення доступу при звільненні працівника**

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

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

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

3. Працівник, що звільняється, має передати матеріальні цінності (пристрої), надані йому в користування/наявні в кабінеті, завідувачу господарством.

4. Інженер-електронік в присутності завідувача господарством 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 не пізніше 5 днів після звільнення працівника.

6. Інженер-електронік, відповідальний за створення корпоративних акаунтів, має видалити обліковий запис працівника, що звільняється, не пізніше наступних 5 днів після звільнення працівника.

7. Інженер-електронік має оновити паролі до усіх інших облікових записів, до яких мав доступ працівник, що звільняється не пізніше наступних 5 днів після звільнення працівника.

### **Збереження інформації**

Для здійснення збереження та захисту даних закладу освіти керівник закладу освіти призначає уповноважених ним осіб, відповідальних за інформаційно-технічне забезпечення закладу освіти.

До функціональних обов'язків уповноважених осіб вноситься запис:

Встановлення, збереження та оновлення паролів на відповідних інформаційних та технічних ресурсах освітнього закладу.

При зміні технічного обладнання уповноважені особи контролюють технічні роботи, заміну та встановлення паролів, ведуть роз'яснювальну роботу серед учасників освітнього процесу про необхідність цифрової безпеки у закладі.

### **Робота з паролями**

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

Для збереження паролів використовується:

- паперовий варіант – зберігається в сейфі адміністрації закладу;
- текстовий документ – зберігається документ в архіві під паролем.

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

**Обслуговування комп'ютерів, які використовуються для спільної роботи** (учнівські комп'ютери, комп'ютер у бібліотеці, в учительській тощо) здійснюється інженером-електроніком.

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

1. Налаштувати захист.
2. Забезпечити коректне використання шкільної мережі Wi-Fi.

3. Налаштувати сканер безпеки на ПК.
4. Прописати правила користування зовнішніми носіями інформації (флеш, карти пам'яті)
5. Слідкувати за оновленнями.
6. Заборонити інсталювати програмне забезпечення з-поза меж організації, яке не затверджено або не адмініструється у закладі.
7. Безпечно зберігати дані.
8. Постійно нагадувати (створювати пам'ятки, викладати їх на видне місце) щодо правил безпеки.

### **Використання специфічних програм**

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

Також в закладі освіти дозволено встановлення та використання комп'ютерних програм в навчанні дітей з особливими освітніми потребами. Типовим переліком допоміжних засобів для навчання (спеціальних засобів корекції психофізичного розвитку) осіб з особливими освітніми потребами, які навчаються в закладах освіти, затвердженого наказом Міністерства освіти і науки України від 23.04.2018 № 414, визначено комп'ютерні програми для ведення корекційної діяльності з дітьми відповідно до нозології та їх специфічного порушення.

### **Функціонування загальної мережі ПК в закладі освіти**

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

Загальна мережа закладу освіти	Назва
Інтернет провайдер закладу освіти	Для підключення ПК до мережі укладено договір з інтернет-провайдером ТОВ «Сіпком Плюс», який забезпечує доступ до Інтернету
Тип підключення закладу освіти до мережі Інтернету	бездротовий Wi-Fi та провідний Ethernet



Налаштування доступу до мережі Інтернету закладу освіти шляхом введення облікових даних, таких як ім'я користувача та пароль	так
Адміністратор мережі закладу освіти	Інженер-електронік
Встановлення рівня доступу до мережі на ПК	Інженер-електронік

В закладі освіти встановлені засоби відеоспостереження.

Пароль доступу до архіву зберігається за прийнятими в закладі освіти правилами, оновлюється один раз на місяць.

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

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

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

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.

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.

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 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.

Сайт закладу освіти функціонує відповідно до статті 30 Закону України «Про освіту» (Прозорість та інформаційна відкритість 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://zs.zp.ua/>.

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

Дизайн сайту формується в рамках наявних можливостей і повинен відповідати цілям, завданням, структурі 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).

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 рекламно-комерційного характеру та інформації, яка не належить до сфери діяльності установи.

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

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

Для захисту сайту закладу освіти потрібно передбачити та забезпечити:

Технічний захист - це аспект безпеки, що стосуються захисту технічних ресурсів та інформаційних технологій від зловживання: захист від кібератак, вірусів, шпигунського ПЗ, шахрайства та інших загроз. Технічна безпека може бути забезпечена шляхом автентифікації користувачів, надання права доступу,

обов'язкового резервного копіювання розміщених матеріалів, антивірусного програмне забезпечення.

Юридичний захист - це аспект безпеки, що стосуються дотримання законодавства в галузі захисту персональних даних, прав на інтелектуальну власність, авторського права, конфіденційності та інших правових питань. Для забезпечення юридичної безпеки, сайт має відповідати вимогам законодавства та політики захисту даних.

При розміщенні інформації на сайті необхідно забезпечувати дотримання вимог законодавства України про захист персональних даних. Всі матеріали про учасників освітнього процесу (керівників, 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 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 квартал.

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

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

Згідно із Законом України «Про захист персональних даних» при зарахуванні дитини до закладу освіти закладом освіти отримується обов'язково задокументована згода суб'єктів персональних даних. Оскільки суб'єктами персональних даних є неповнолітні особи, то згідно з нормами Сімейного та Цивільного кодексів України, згоду на обробку персональних даних дитини мають надати батьки або особи, які їх замінюють. Також батьки повинні подати

згоду на обробку власних персональних даних. Із настанням повноліття особа надає таку згоду самостійно, і батьки вже не мають права визначати межі обігу персональних даних їхніх дітей.

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

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

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

З урахуванням обмежень, визначених законодавством, допускається відкрита зйомка на вулиці, на публічних заходах, здійснення відео- та фотозйомки навчальних занять, розміщення цих матеріалів на офіційних ресурсах закладу освіти без зазначення персональних даних учнів, вчителів, локації (останнє – 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 2 статті 32 Конституції України, відповідно до яких збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди можливі, зокрема в інтересах прав людини.

З метою дотримання авторського права матеріали (наприклад, відеозапис або презентація 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 для закладу освіти є одним із способів комунікації між всіма учасниками освітнього процесу.

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

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

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

Визначено електронну пошту (ел.пошта) закладу освіти: `mzk.zsich1@gmail.com`.

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

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

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

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

У разі звільнення працівника, електронна скринька таких користувачів ліквідується.

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

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

Працівники закладу освіти зобов'язані використовувати корпоративну електронну пошту при здійсненні своїх посадових обов'язків, зокрема, відправляти та отримувати електронне листування внутрішнім і зовнішнім кореспондентам з використанням адреси робочої пошти.

Працівник закладу освіти не має права:

- а) використовувати електронну пошту закладу для цілей, не пов'язаних з виконанням посадових обов'язків в закладі освіти;
- б) повідомляти пароль доступу до адреси скриньки іншим особам;
- в) здійснювати масову розсилку листів зовнішнім адресатам, в тому числі листів рекламного характеру;

г) розсилати листи, що містять:

- конфіденційну інформацію, доступ до якої обмежено чинним законодавством, у тому числі містить державну таємницю, матеріали, використання яких порушує права власності;

- недостовірну інформацію, а також інформацію, що ображає честь і гідність осіб, ганьбить ділову репутацію, пропагує ненависть або дискримінацію людей за расовими, етнічними, статевими, релігійними, соціальними ознаками, закликає до протиправних дій;

- матеріали, що містять віруси або інші комп'ютерні коди; файли, програми, призначені для порушення, знищення або обмеження функціональності будь-якого комп'ютерного обладнання.

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

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

В закладі освіти мережева комунікація здійснюється в Facebook.

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, 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; не використовуються соціальні мережі та пошукові системи (у т.ч. із застосуванням сервісів VPN), доступ до яких обмежено відповідно до Указу Президента України «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

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

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

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

Спільноти, сформовані для комунікації та різного роду інформування учасників освітнього процесу, класифікуються за призначенням: для інформування учасників освітнього процесу про новини закладу освіти; для спілкування педагогічних працівників з адміністрацією; для спілкування вчителів та учнів класу чи паралелі; для обміну інформацією між вчителем та батьками класу та інші.

Створюються закриті спільноти – 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 для учнів, прийнятих в закладі освіти (Додаток 2).

Презентація закладу освіти в соцмережах, здійснення спілкування його працівників в месенджерах має бути коректним, професійним, етичним. Працівники закладу освіти мають усвідомлювати ризики втрати онлайн-репутації – власної та закладу освіти.

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

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

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 організації освітнього процесу з використанням технологій дистанційного навчання в ЗНВК «Запорізька Січ» (Протокол педради від 21.08.2023 №1, наказ від 21.08.2023 №55/р), якою узгоджено правила та алгоритми взаємодій усіх учасників освітнього процесу для виконання освітніх програм закладу в даному форматі надання освітніх послуг.

Для організації дистанційного формату навчання в закладі освіти визначено онлайн- платформи - 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 (ZOOM, GoogleMeet) в закладі освіти для здобувачів освіти різних вікових категорій.

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

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

В закладі освіти використовується захищена та надійна шкільна мережа: використовуються послуги офіційного інтернет-провайдера ТОВ «Сіпком Плюс», встановлено програмне забезпечення для фільтрації та моніторингу безпеки пристроїв.

В разі використання вчителями та учнями під час дистанційного навчання особистих домашніх пристроїв, які зазвичай не охоплюються мережевим

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.

Закладом освіти проводяться заходи щодо дотримання авторського права.

Відповідно до Положення про академічну доброчесність учасників освітнього процесу ЗНВК «Запорізька Січ» (погодженого педагогічною радою, протокол від 05.01.2021 №5; затвердженого наказом від 05.01.2021 № 2) в закладі освіти забезпечується дотримання академічної доброчесності всіма учасниками освітнього процесу.

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

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

Також аналізуються платформи, інтернет-ресурси, на яких учителями розміщуються навчальні матеріали або на які учням надається покликання для виконання завдань, на предмет наявності на таких ресурсах небажаного

контенту для заміни в разі необхідності платформи для розміщення матеріалів, здійснення учасниками освітнього процесу дій щодо блокування реклами, інш.

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

- негайне інформування відповідальної особи або керівника закладу освіти про інцидент, пов'язаний з безпекою дітей, що виник в цифровому середовищі, для прийняття рішення щодо подальших дій: інформування батьків дитини, відповідних служб та установ правопорядку про встановлені порушення прав дитини;

- збереження (фіксація) ознак інциденту, у т.ч на матеріальних носіях;

- забезпечення захисту інформаційних ресурсів закладу освіти;

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

В закладі освіти прийнято правила (вимоги) проведення дистанційного (онлайн) заняття: визначені умови підключення учнів 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.

Про дотримання цих правил інформуються всі учасники освітнього процесу.

В закладі освіти встановлюються умови та правила використання мобільних технологій та інших електронних пристроїв під час навчальних занять (Додаток 3).

Умови та правила використання мобільних технологій та інших електронних пристроїв в закладі освіти обговорюються та приймаються колективно, про дотримання цих правил інформуються всі учасники освітнього процесу.

## **VIII РОЗДІЛ. Захист персональних даних в цифровому середовищі закладу освіти**

Відповідно до Закону України «Про захист персональних даних» під час прийняття на роботу працівника, зарахування здобувача освіти до закладу освіти, подання відповідної заяви батьками здобувача освіти оформлюється згода суб'єкта персональних даних (батьки здобувачів освіти, працівники

закладу освіти) шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки.

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

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

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

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

## **IX РОЗДІЛ. Прикінцеві положення**

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

Порядок обговорення оновлень визначається педагогічною радою.

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

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

На період дії правового режиму воєнного стану застосовуються обмеження в публікації інформації, інших даних, визначених органами законодавчої влади, закладом освіти.

## Додаток 1

### **Загальні настанови та рекомендації щодо налаштувань і доступів до мережі:**

#### **1. Пароль і безпека:**

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

Регулярно оновлюйте паролі і уникайте використання слабких або очевидних паролів.

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

#### **2. Оновлення програмного забезпечення:**

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

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

#### **3. Захист від шкідливих програм.**

Встановіть надійне антивірусне програмне забезпечення та антивірусні програми.

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

Уникайте відкриття підозрілих посилань або вкладень в електронних листах.

#### **4. Налаштування мережі:**

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

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

#### **5. Керування обліковими записами:**

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

## Додаток 2

### Правила спілкування в чатах

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, трансліуйте 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.



### Додаток 3

#### **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 медіаграмотості.

З метою запобігання порушень дисципліни під час освітнього 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, інші девайси, гаджети за умови безпеки цих пристроїв, відсутності загрози для життя і безпеки 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, 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 освіти або за певних умов;

Використання мобільного гаджету (смартфону) не рекомендується:

- учням початкової школи впродовж перебування в закладі освіти (за виключенням виконання навчального завдання (за умов 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 пристрою забороняється:

- під час уроку без прямого дозволу вчителя на використання пристрою в чітко визначений час та умови використання для виконання освітньої задачі ;

- для здійснення фото- чи відеозйомки 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 на засіданні Ради профілактики правопорушень закладу освіти (за участю батьків здобувача освіти).