ЗАТВЕР
Директор Запо
академічного лі
Запорізької міс
Запорізько



Володимир МА

наказом № 106 р від 15.0

ПОЛОЖЕННЯ

Про цифрову безпеку закладу освіти Запорізького академічного ліцею № 23 Запорізької міської ради Запорізької області

(схвалено педагогічною
протокол № 1 від 15.08.2

1. Загальні положення

1.1. Це Положення визначає систему організаційних, технічних, педагогічних та правових заходів, спрямованих на забезпечення цифрової безпеки, захист інформаційних ресурсів, персональних даних та безпечного використання цифрових технологій в Запорізькому академічному ліцеї № 23 Запорізької міської ради Запорізької області (далі — Ліцей № 23).

1.2. Положення є обов’язковим для виконання всіма учасниками освітнього процесу: педагогічними та іншими працівниками Ліцею № 23, учнями, батьками (законними представниками), а також особами, які тимчасово перебувають у Ліцеї № 23 та мають доступ до його цифрових ресурсів.

1.3. Цифрова безпека в Ліцеї № 23 є складовою загальної системи безпеки освітнього середовища та спрямована на:

- захист прав і свобод людини в цифровому просторі;
- запобігання кіберзагрозам та інцидентам;
- формування культури безпечної цифрової поведінки;
- забезпечення безперервності освітнього процесу.

1.4. Дія цього Положення поширюється на:

- комп’ютерну техніку та інші цифрові пристрої Ліцею № 23;
- локальну мережу та доступ до мережі Інтернет;
- освітні платформи, електронні журнали, хмарні сервіси;
- офіційні веб ресурси та сторінки Ліцею № 23;
- персональні дані учасників освітнього процесу.

1.5. Положення затверджується наказом директора Ліцею № 23 та набирає чинності з дня його введення в дію.

2. Нормативно-правова база

2.1. Положення розроблено відповідно до чинного законодавства України, зокрема:

- Конституції України;
- Закону України «Про освіту»;
- Закону України «Про повну загальну середню освіту»;
- Закону України «Про захист персональних даних»;
- Закону України «Про інформацію»;
- Закону України «Про основні засади забезпечення кібербезпеки України»;
- Закону України «Про електронні комунікації»;
- Концепції розвитку цифрових компетентностей;
- Державного стандарту базової і повної загальної середньої освіти;
- інших нормативно-правових актів у сфері освіти, інформаційної та кібербезпеки.

2.2. У разі внесення змін до законодавства України норми цього Положення застосовуються в частині, що не суперечить чинному законодавству.

2.3. Ліцей № 23 у сфері цифрової безпеки керується також наказами засновника, рекомендаціями Міністерства освіти і науки України та внутрішніми розпорядчими документами.

3. Терміни та визначення

У цьому Положенні терміни вживаються в такому значенні:

3.1. **Цифрова безпека** — стан захищеності цифрового освітнього середовища, інформаційних ресурсів і персональних даних від внутрішніх та зовнішніх загроз.

3.2. **Інформаційна безпека** — комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, втрати, спотворення або знищення.

3.3. **Персональні дані** — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована.

3.4. **Кіберінцидент** — подія або сукупність подій, що призводять або можуть призвести до порушення конфіденційності, цілісності чи доступності інформації.

3.5. **Освітні цифрові ресурси** — електронні платформи, сервіси, програмне забезпечення, що використовуються для організації освітнього процесу.

3.6. **Кібергігієна** — сукупність правил та навичок безпечної поведінки користувача в цифровому середовищі.

4. Мета та завдання цифрової безпеки Ліцею № 23

4.1. Метою цифрової безпеки в Ліцеї № 23 є створення безпечного, надійного та контрольованого цифрового освітнього середовища, що забезпечує захист інформації, персональних даних та прав учасників освітнього процесу.

4.2. Основними завданнями цифрової безпеки є:

- запобігання несанкціонованому доступу до цифрових ресурсів Ліцею ;
- захист персональних даних учнів і працівників;
- формування безпечної цифрової поведінки;
- підвищення рівня цифрової грамотності;
- мінімізація ризиків кіберзагроз;
- забезпечення стабільної роботи освітніх цифрових сервісів.

4.3. Реалізація завдань цифрової безпеки здійснюється шляхом:

- упровадження внутрішніх правил і процедур;
- технічного захисту інформаційних систем;
- проведення навчань, інструктажів та профілактичних заходів;
- контролю та моніторингу дотримання вимог цього Положення.

5. Суб’єкти цифрової безпеки та їх повноваження

5.1. Суб’єктами забезпечення цифрової безпеки в Ліцеї № 23 є:

- директор Ліцею № 23;
- заступники директора відповідно до розподілу обов’язків;
- педагогічні працівники;
- працівники, відповідальні за інформаційно-комунікаційні технології;
- учні Ліцею № 23;
- батьки або законні представники учнів.

5.2. **Директор Ліцею № 23**:

- забезпечує загальне керівництво системою цифрової безпеки;
- затверджує внутрішні нормативні документи з питань цифрової безпеки;
- визначає відповідальних осіб за організацію та контроль цифрової безпеки;
- створює умови для захисту інформаційних ресурсів та персональних даних;
- несе персональну відповідальність за стан цифрової безпеки в Ліцеї № 23.

5.3. **Заступники директора**:

- організовують виконання вимог цього Положення у межах своїх повноважень;
- координують роботу педагогічних працівників щодо безпечного використання цифрових технологій;
- забезпечують контроль за дотриманням правил цифрової безпеки під час освітнього процесу.

5.4. **Педагогічні працівники**:

- дотримуються вимог цього Положення;
- використовують лише дозволені освітні цифрові ресурси;
- забезпечують захист персональних даних учнів;

- формують в учнів навички безпечної цифрової поведінки;
- негайно інформують адміністрацію про виявлені кіберінциденти.

5.5. **Відповідальні за ІКТ працівники**:

- забезпечують технічний захист цифрових систем;
- здійснюють налаштування доступу до мережі та сервісів;
- проводять резервне копіювання даних;
- здійснюють моніторинг кіберзагроз.

5.6. **Учні Ліцею № 23** зобов'язані:

- дотримуватися правил безпечної поведінки в цифровому середовищі;
- не поширювати конфіденційну інформацію;
- не використовувати заборонене програмне забезпечення;
- негайно повідомляти педагогів про загрози або підозрілі ситуації.

5.7. **Батьки (законні представники)**:

- сприяють формуванню в учнів відповідального ставлення до цифрових технологій;
- дотримуються вимог захисту персональних даних;
- взаємодіють із Ліцеєм № 23 у питаннях цифрової безпеки.

6. Захист персональних даних учасників освітнього процесу

6.1. У Ліцеї № 23 здійснюється обробка персональних даних виключно з метою забезпечення освітнього процесу та відповідно до законодавства України.

6.2. До персональних даних належать:

- відомості про учнів та їхніх батьків;
- персональні дані працівників Ліцею № 23;

- інформація, що міститься в електронних журналах, базах даних, особових справах.

6.3. Обробка персональних даних здійснюється на засадах:

- законності;
- цільового призначення;
- мінімізації обсягу даних;
- конфіденційності та захищеності.

6.4. Забороняється:

- передача персональних даних третім особам без законних підстав;
- зберігання персональних даних на несанкціонованих носіях;
- використання особистих акаунтів для обробки службової інформації.

6.5. Доступ до персональних даних мають лише уповноважені особи відповідно до службових обов’язків.

6.6. У разі виявлення порушень захисту персональних даних адміністрація Ліцею зобов’язана вжити невідкладних заходів щодо їх усунення.

7. Інформаційна безпека освітніх платформ та цифрових ресурсів

7.1. У Ліцеї № 23 використовуються лише ті цифрові освітні платформи та сервіси, які відповідають вимогам законодавства України та забезпечують належний рівень інформаційної безпеки.

7.2. Для доступу до освітніх цифрових ресурсів використовуються персональні облікові записи з обмеженими правами доступу.

7.3. Забороняється:

- використання неліцензійного програмного забезпечення;
- встановлення сторонніх програм без погодження з адміністрацією;
- передача облікових даних третім особам.

7.4. Освітні платформи повинні забезпечувати:

- захист від несанкціонованого доступу;
- збереження цілісності інформації;
- можливість резервного копіювання.

7.5. Адміністрація Ліцею № 23 здійснює періодичний перегляд переліку дозволених цифрових ресурсів.

8. Правила користування мережею Інтернет у Ліцеї № 23

8.1. Доступ до мережі Інтернет у Ліцеї № 23 надається з метою забезпечення освітнього процесу, адміністративної діяльності та професійного розвитку працівників.

8.2. Користування мережею Інтернет здійснюється відповідно до цього Положення, правил внутрішнього трудового розпорядку та чинного законодавства України.

8.3. Забороняється використання мережі Інтернет для:

- перегляду та поширення матеріалів, що містять насильство, дискримінацію, пропаганду війни, жорстокості або порнографії;
- порушення авторських прав;
- участі в кібербулінгу, шахрайстві чи інших протиправних діях;
- встановлення програмного забезпечення без дозволу адміністрації.

8.4. Ліцей № 23 має право застосовувати технічні засоби фільтрації та обмеження доступу до небажаних вебресурсів.

8.5. Використання особистих пристроїв учнів під час освітнього процесу допускається лише з дозволу педагогічного працівника та з освітньою метою.

9. Кібергігієна та цифрова поведінка учасників освітнього процесу

9.1. У Ліцеї № 23 формується культура відповідальної та безпечної цифрової поведінки.

9.2. Учасники освітнього процесу зобов’язані:

- використовувати складні паролі та не передавати їх іншим особам;
- регулярно оновлювати програмне забезпечення;
- не відкривати підозрілі файли та посилання;
- дотримуватися етичних норм спілкування в цифровому середовищі.

9.3. Учні Ліцею № 23 повинні:

- поважати права інших користувачів;
- не поширювати неправдиву або образливу інформацію;
- повідомляти педагогів про випадки кібербулінгу чи цифрових загроз.

9.4. Педагогічні працівники зобов’язані:

- бути прикладом безпечної цифрової поведінки;
- інтегрувати питання кібергігієни в освітній процес;
- проводити роз’яснювальну роботу з учнями та батьками.

10. Реагування на інциденти цифрової та кібербезпеки

10.1. У разі виявлення кіберінциденту будь-який учасник освітнього процесу зобов’язаний негайно повідомити адміністрацію Ліцею № 23.

10.2. До кіберінцидентів належать:

- несанкціонований доступ до цифрових ресурсів;
- витік персональних даних;
- зараження комп’ютерної техніки шкідливим програмним забезпеченням;
- спроби фішингу або кібершахрайства.

10.3. Адміністрація Ліцею № 23:

- фіксує факт кіберінциденту;
- вживає заходів щодо локалізації та усунення наслідків;

- за потреби інформує відповідні органи.

10.4. За результатами розгляду кіберінциденту можуть бути застосовані заходи дисциплінарного впливу відповідно до законодавства.

11. Навчання та підвищення цифрової грамотності

11.1. Ліцей № 23 забезпечує систематичне навчання працівників та учнів з питань цифрової безпеки.

11.2. Навчання здійснюється шляхом:

- проведення інструктажів;
- організації семінарів і тренінгів;
- участі в освітніх програмах та проєктах з цифрової грамотності.

11.3. Учні Ліцею № 23 залучаються до профілактичних заходів щодо безпечної поведінки в Інтернеті.

12. Моніторинг, контроль та відповідальність

12.1. Контроль за дотриманням цього Положення здійснює директор Ліцею № 23 та уповноважені особи.

12.2. Моніторинг стану цифрової безпеки проводиться шляхом:

- аналізу використання цифрових ресурсів;
- перевірки дотримання вимог безпеки;
- розгляду звернень та скарг.

12.3. Особи, винні у порушенні вимог цього Положення, несуть відповідальність згідно з чинним законодавством України.

13. Прикінцеві положення

13.1. Це Положення вводиться в дію наказом директора Ліцею № 23

13.2. Зміни та доповнення до Положення вносяться наказом директора відповідно до чинного законодавства.

13.3. Положення доводиться до відома всіх учасників освітнього процесу під підпис або шляхом оприлюднення на офіційному вебресурсі Ліцею № 23.