**СРЕДНО УЧИЛИЩЕ "ВАСИЛ ЛЕВСКИ", ГРАД ДОЛНИ ЧИФЛИК**
гр. Долни чифлик, област Варна, ул. "Трети март" 15, тел.: 051422765, e-mail: info-400126@edu.mon.bg

# ПРАВИЛА ЗА РАБОТА С ИНФОРМАЦИОННИТЕ СИСТЕМИ/ТЕХНОЛОГИИ в СУ„ВАСИЛ ЛЕВСКИ“, град ДОЛНИ ЧИФЛИК

## Глава първа
## Общи положения

**Чл. 1.** (1) Правилата за използване на информационните системи информират педагогическите специалисти и непедагогическия персонал в образователната институция за правата и задълженията им по отношение на работата с информационните системи/технологии.

(2) Правилата определят правилата за използване на информацията за вътрешна и външна комуникация, за предоставяне на услуги на родители и учители, за администриране, свързано с образователния процес, а също така е средство за извършване на проучвания и обмяна на информация.

(3) Достъпът до данните в локалната мрежа и ползването на програмните продукти на институцията от педагогическите специалисти и непедагогическия персонал е необходимо с оглед ефективното изпълнение на отговорностите и задълженията.

(4) Правата за достъп са две основни групи – потребителски и администраторски. Администраторските права на достъп се определят със заповед на директора на институцията.

**Чл. 2.** Информационните технологии включват локалните мрежи, интернет, електронната поща и всички програмни продукти, които образователната институция притежава и използва.

**Чл. 3.** Правилата дават указания за начина на употреба от педагогическите специалисти и непедагогическия персонал на информационните технологии, насърчава ползването им с цел увеличаване на продуктивността и ефективността на работата.

**Чл. 4.** Определеният заместник-директор, ръководителят на направление „Информационни и комуникационни технологии“/ и специалистът по IT технологии в образователната институция са отговорни за цялостната дейност на информационните технологии и за подпомагането работата на персонала с тях.

**Чл. 5.** Работниците и служителите в образователната институция са задължени да спазват правилата.

**Чл. 6.** Всички компютърни програмни продукти и информация, създадена и съхранена от работниците/служителите, са собственост на институцията.

**Чл. 7.** Работниците/служителите в институцията нямат право да вземат програмни продукти с цел инсталацията им на домашните им компютри и преносими устройства, с изключение на електронни учебници/познавателни книжки и създадените за он-лайн обучение софтуери.

**Чл. 8.** При напускане на институцията, работниците/служителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

## Глава втора
## Контрол върху работата с информационните технологии

**Чл. 9.** (1) Ръководството на институцията има право да контролира ползването на програмните продукти, електронната поща, Интернет и базите данни, създадени от педагогическите специалисти и непедагогическия персонал в образователната институция.

(2) Ръководството на образователната институция има право да проверява изцяло служебните компютри, предоставени за учебни цели на персонала в институцията, както и техниката, която ползват учители и служители във връзка с изпълнение на служебните им задължения.

## Глава трета
## Конфиденциалност

**Чл. 10. (1)** Конфиденциалността на информацията е лична отговорност на всеки, чийто профил осигурява достъп до нея, в съответствие с предоставените му права.

**(2)** Резултатите от извършения контрол върху работата с информационните технологии на образователната институция се считат за конфиденциални и не се разгласяват от ръководството.

## Глава четвърта
## Допустимо ползване на информационните технологии за лични цели

**Чл. 11.** Учебните информационни системи са предназначени за ползване при изпълняване на служебните задължения на работниците/служителите.

**Чл. 12.** Тези системи могат да се ползват и за лични цели при следните условия:

1. Инцидентно, рядко и за кратко време.
2. Не е по време на работа, а е в извънработно време.
3. Това не пречи на работата на останалите работници/служители. В това число се включват дейности, които могат да доведат до конфликт на интереси.
4. Това не води до допълнителни разходи за институцията.

## Глава пета
## Забрана за ползване на информационните технологии

**Чл. 13.** Този списък на забранените дейности във връзка с информационните технологии не е изчерпателен и към него може да се добавят допълнителни забрани със заповед на директора.

**Чл. 14.** Забранява се ползването на компютърните и информационните системи на образователната институция в следните случаи:

1. Заобикаляне на системите за сигурност, с цел разрушаване или намаляване сигурността на учебната локална мрежа или бази данни.
2. Ползване на компютърните ресурси за извършване на престъпление.
3. Използване на ресурсите за подпомагане дейността на дадена компания, нейните продукти, услуги или бизнес практика.
4. Електронната поща на институцията не може да се ползва за комерсиални лични цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на образователната институция.
5. Ползването на компютърните системи за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат.

6. Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, пращани от персонала трябва да са лично подписани.
7. Свалянето от Интернет на аудио и видео файлове.
8. Сваляне и инсталиране на компютърни програми от Интернет без разрешение на компютърните специалисти.
9. Копиране на лицензираните компютърни програми на институцията с цел лична употреба.

## Глава шеста
## Разкриване на информация

**Чл. 15.** (1) Неоторизираното разкриване на служебна информация може да доведе до негативни последици за образователната институция и накърняване на нейния имидж и репутация.

(2) Работник/служител, който е копирал и използвал информация от локалната мрежа на институцията за лична изгода или за да причини вреда на институцията, носи съответната дисциплинарна и имуществена отговорност по Кодекса на труда.

## Глава седма
## Антивирусна защита

**Чл. 16.** (1) Компютърните вируси са голяма заплаха за всички потребители на IT услуги и работниците и служителите трябва да имат необходимите знания как вирусите се разпространяват, каква вреда могат да нанесат и как да се предпазват от тях.

(2) Компютърният вирус е компютърна програма, която се задейства на даден компютър и се разпространява към другите дискове и програми, които са в контакт със заразения компютър.

(3) Вирусът може да причини блокиране на компютъра, да промени бази данни, да направи някои данни невъзможни за ползване и даже да форматира диск и така да се загуби цялата записана информация.

**Чл. 17.** (1) IT специалистът на образователната институция носи пълната отговорност за избирането и инсталирането на антивирусната програма, както и за нейната актуализация на всеки индивидуален компютър. Служителите също трябва да следят дали тяхната антивирусна програма се осъвременява периодично с най-новата версия.

(2) Работниците/служителите трябва да приемат всяко съобщение за вирус изключително сериозно и да следват вътрешните процедури за реакция в такъв случай.

(3) Преднамереното разпространяване на данни, за които работникът/служителят знае, че са заразени с вирус е нарушение на служебните задължения, което се санкционира по дисциплинарен ред.

(4) В случай на вирусна атака работникът/служителят трябва незабавно да информира IT специалиста, без да предприема никакви действия самостоятелно.

(5) Входящата електронна поща трябва да се третира с особено внимание поради потенциалната възможност да е заразена с вируси. Отварянето на приложения да се прави само след предварителното им сканиране с антивирусна програма.

(6) Ползването на външни носители (дискове, външна памет и др.) на информация е допустимо само след предварителното им сканиране с антивирусна програма.

## Глава осма

## Архивиране на информацията и възстановяване

**Чл. 18.** (1) Сривовете в компютърното оборудване, вирусите и случайното изтриване на файлове могат да причинят загуба на данни, поради което е необходимо информацията във всяка компютърна система да бъде архивирана.

(2) Целта на архивирането е да се възстанови работата възможно най-бързо в случай на прекъсване по технически причини. По този начин се минимизират възможните проблеми и загуби.

(3) Работниците/служителите в институцията, съгласувайки с IT специалиста, трябва да имат адекватна система за архивиране на данните от своята работа на технически носители (дискове, USB и др.).

(4) Честотата на архивирането се определя от директора в писмена процедура и зависи от броя транзакции и тяхната значимост за системата.

(5) Задължително архив (архивиране на файлове) се прави веднъж месечно.

(6) Направените архивни копия се съхраняват по възможност в специално предназначен за целта заключен шкаф.

(7) Архивните копия се обозначават със следните данни:

1. име на информацията;
2. дата на създаване;
3. срок на съхранение;
4. име на служителя, извършил архивирането.

(8) Архивните копия се проверяват периодично за пълнота на архивираната информация и възможност за възпроизвеждането ù.

(9) При срив в информационните системи, специалистът по информационни технологии предприема нужните действия за възстановяване на нормалното функциониране на системите. При загуба или повреждане на информация, я възстановява, като използва последното актуално архивно копие.

## Глава девета

## Достъп и пароли

**Чл. 19.** (1) Работниците/служителите получават достъп до локалната мрежа и до всички програми, необходими за изпълнение на служебните им задължения.

(2) Достъпът до дадена програма се дава на конкретен работник/служител и не може да се прехвърля на друг.

(3) Работниците/служителите трябва да пазят своите лични пароли в тайна.

(4) Когато даден продукт изисква парола, следва да се спазват следните правила:

1. служителят трябва да промени първоначалната парола, обикновено генерирана от програмния продукт, като измисли своя;
2. паролите следва да съдържат малки и големи букви, цифри и специални символи, дължината им трябва да е не по-малко от 8 символа за потребителските и 12 символа за администраторските профили, но лесно да се помнят, за да не се налага записване на хартиен носител и да се оставят на работното място;
3. желателно е паролите да се сменят на определена честота (3, 6 месеца), като при периодична промяна, не е желателно да се ползват вече използвани пароли.

## Глава десета
## Интернет

**Чл. 20.** (1) Ръководството насърчава ползването на Интернет от работниците/служителите за обмяна на информация, извършване на проучвания и събиране на данни във връзка с дейността им.

(2) Заместник-директорите и други оторизирани длъжностни лица отговарят за уместната употреба на Интернет от персонала.

## Глава единадесета
## Електронна поща

**Чл. 21.** (1) Електронната поща на институцията не може да се ползва за комерсиални и религиозни цели или да се подпомага бизнес, който не е свързан с дейността на институцията.

(2) Ползването на електронната поща за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат също не се позволява.

(3) Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност се забранява. Всички електронни писма, изпращани от работниците/служителите трябва да са лично подписани.

(4) Всички електронни писма и важни съобщения, които имат отношение към дейността на образователната институция, трябва да се принтират и представят за завеждане с входящ номер в Дневника за входяща кореспонденция от определеното длъжностно лице, като екземпляр се съхранява в съответните класьор и в електронната поща.

## Глава дванадесета
## Лице за контакт

**Чл. 22.** Всички технически въпроси във връзка с работата на компютърните системи се насочват към IT специалиста на образователната институция или към друго лице, определено от директора.

## Допълнителни разпоредби

**§ 1.** При извършване на самооценката на вътрешните контроли следва да се направи анализ и оценка на риска на критичните информационни системи в образователната институция.

**§ 2.** Целта е да е идентифицират най-важните компоненти (оборудване, програми, бази данни и др.), заплахата за тяхната повреда или загуба, последиците от това за дейността на институцията, за да се предотвратят потенциалните проблеми, както и да се въведат допълнителни контроли, които са необходими за подобряване на системата.

**§ 3.** Оценката на риска обхваща извършеното, както и моментното състояние, мерките за подобряване на слабите места във вътрешните контроли, необходимите ресурси и остатъчния риск за институцията, който контролите няма как да елиминират.

**§ 4.** При създаването на програмен продукт специално за нуждите на институцията е необходимо още при задаването на неговите параметри на доставчика да се заложат основните контролни функции, които този продукт трябва да има.

**Заключителни разпоредби**

**§ 1.** Настоящите правила са обект на изменения и допълнения, когато те служат за подобряване на ефективността на изпълнението им и/или третират проблеми, останали незасегнати в тях.

**§ 2.** Настоящите правила са приети с Решение № 30, взето с Протокол № РД-05-11/11.09.2023 г. от заседание на Педагогическия съвет.

**ДИРЕКТОР:**.....
Д. Янева