



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. “Княгиня Евдокия” №41
e-mail: info-1600116@edu.mon.bg

тел/факс: 0331/6 47 87
<http://www.susskm.com>

ЗАПОВЕД № РД-10-806/15.12.2025 г.

На основание чл. 258, ал. 1, чл.259, ал.1 и чл.28, ал.1, т. 2 Закона за предучилищното и училищното образование, чл. 31, ал. 1, 6 от Наредба № 15/ 2019 г. за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти

1. УТВЪРЖДАВАМ:

Правила за мрежова и информационна сигурност на СУ „Св. св. Кирил и Методий“, град Асеновград

2. ОПРЕДЕЛЯМ:

Г-н Л. Костов за системен администратор на мрежовата и информационна сигурност в училище.

Л. Костов изпълнява своите задължения, съгласно утвърдените Правила за мрежова и информационна сигурност

Контрол по изпълнение на заповедта възлагам г-жа В. Филипова, ЗД по УД.

МАЯ КРАЕВА

Директор на СУ „Св. св. Кирил
и Методий“ гр. Асеновград

В. Филипова
Л. Костов



Утвърдил:

Директор:

/Мая Краева/



Правила за мрежова и информационна сигурност

**СУ "СВ. СВ. КИРИЛ И
МЕТОДИЙ" гр. Асеновград**



СРЕДНО УЧИЛИЩЕ "СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ" АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

Съдържание	
РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ	2
РАЗДЕЛ II. ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ	3
РАЗДЕЛ III. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ	5
РАЗДЕЛ IV. ПРАВИЛА ЗА РАБОТНОТО МЯСТО И ОТГОВОРНОСТИ НА ПОТРЕБИТЕЛИТЕ	7
РАЗДЕЛ V. МРЕЖОВА СИГУРНОСТ И ПОЛИТИКИ ЗА ИНТЕРНЕТ	9
1. Мрежова структура и контрол	9
2. Защитна стена и интернет филтриране	9
3. Wi-Fi сигурност	10
4. Антивирусни и защитни решения	10
5. Обработка и логване на събития	10
РАЗДЕЛ VI. ПЛАН ЗА РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ	11
РАЗДЕЛ VII. АРХИВИРАНЕ И ВЪЗСТАНОВЯВАНЕ	13
РАЗДЕЛ VIII. ОБУЧЕНИЕ И ПОВИШАВАНЕ НА КВАЛИФИКАЦИЯТА	14
РАЗДЕЛ IX. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ	15
РАЗДЕЛ X. ПРИЛОЖЕНИЯ	16
Приложение 1 – Регистър на техниката	16
Приложение 2 – Регистър за поддръжка	16
Приложение 3 – Инструктаж за ученици	16
Приложение 4 – Регистър за достъп	16
Приложение 5 – Декларация за спазване на правилата	16
Приложение 6 – Формуляр за докладване на инцидент	16
Приложение 7 – Чеклист за проверка на сигурността	17



СРЕДНО УЧИЛИЩЕ „СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ“ АСЕНОВГРАД

ул. „Княгиня Евдокия“ №41
email: info-1600116@edu.mon.bg

☎ тел/факс: 0331/64787
<http://www.susskm.com>

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите Вътрешни правила се утвърждават на основание Наредбата за минималните изисквания за мрежова и информационна сигурност (ПМС № 186 от 26.07.2019 г., отм. ДВ. бр. 42 от 2023 г., но запазващи приложимост в контекста на цялостната сигурност), както и изискванията на ОРЗД (GDPR). Правилата имат за цел осигуряване на контрол, управление, защита и устойчивост на информационните системи, мрежите и данните в СУ „Св. св. Кирил и Методий“ – Асеновград, включително компютърните кабинети, административните системи и електронния дневник.

Чл. 2. „Информационна система“ означава съвкупност от хардуер, софтуер, данни, комуникационно оборудване и обслужващ персонал, използвани за обработване, съхраняване и предаване на информация в училището.

Чл. 3. Всеки служител, ученик и потребител е длъжен да познава и стриктно да спазва настоящите Правила и всички свързани с тях процедури, като носи **лична отговорност** за действията си в информационните системи и мрежи на училището.

Чл. 4. Изграждането, внедряването и поддръжката на информационни системи се извършва при спазване на техническите и организационните изисквания на Наредбата за минималните изисквания за мрежова и информационна сигурност. Управлението, движението и състоянието на компютърната техника се водят в **Регистър на техниката съгласно Приложение 1**. Всички ремонти, профилактика и подмяна на компоненти се вписват в **Регистър за поддръжка съгласно Приложение 2**, които се съхраняват в администрацията на училището.



СРЕДНО УЧИЛИЩЕ "СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ" АСЕНОВГРАД

ул. "Княгиня Евдокия" □41
email: info-1600116@edu.mon.bg

☎ тел/факс: 0331/64787
http://www.suskm.com

РАЗДЕЛ II. ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ

Чл. 5. Директорът на СУ „Св. св. Кирил и Методий“ – Асеновград утвърждава настоящите правила и носи обща отговорност за тяхното прилагане.

Чл. 6. Със заповед на директора се определя **Длъжностно лице по сигурността (ДЛС)**, което:

- координира прилагането на правилата;
- следи за спазването им от служители и ученици;
- е основна контактна точка при инциденти;
- уведомява компетентните органи при сериозни нарушения или пробиви.

Чл. 7. Системният администратор отговаря за:

- техническата поддръжка на мрежата и системите;
- контрол на достъпа до компютърните кабинети, електронния дневник и административните системи;
- водене на регистрите за техника, поддръжка и достъп;
- архивиране и възстановяване на данни.

Чл. 7а. Системният администратор може да бъде вътрешен служител на училището или външна фирма, определена със заповед на директора. В случай на външна фирма, задълженията и сроковете за реакция се уреждат в договор, като училището осигурява лице за контакт, което координира комуникацията и документирането на дейностите.

Чл. 8. Учителите са длъжни:

- да използват служебните системи само за учебни и административни цели;
- да докладват незабавно при инциденти или нередности;
- да инструктират учениците за правилата при работа в компютърните кабинети = Приложение 3.

Чл. 9. Учениците са длъжни:

- да използват училищната мрежа и устройства само за учебни цели;
- да спазват правилата за интернет и информационна сигурност;



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

Тел/факс: 0331/64787
<http://www.susskm.com>

- да не инсталират софтуер или да променят настройки на училищните компютри;
- да докладват при забелязани проблеми или инциденти.

Чл. 10. Обучение и информираност:

- Всеки служител преминава задължително начално и ежегодно обучение по мрежова и информационна сигурност.
- Учениците преминават кратък инструктаж в началото на всяка учебна година.
- Обученията включват теми като: разпознаване на фишинг, социално инженерство, работа с лични данни (GDPR), процедури при инцидент.



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

РАЗДЕЛ III. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 11. Защитата на информационните системи се основава на следните принципи:

- разделяне на потребителски и администраторски права;
- определяне на нива на достъп според длъжността;
- регистриране (логване) на достъпа, промяната и заличаването на данни;
- използване на техниката изключително за служебни и учебни цели;
- забрана за инсталиране на софтуер от потребители без разрешение на системния администратор;
- забрана за ползване на неоторизиран хардуер и софтуер;
- при употреба на външни носители – задължително предварително сканиране с антивирусен софтуер;
- забрана външни лица да имат достъп до комуникационния шкаф и мрежовото оборудване;
- забрана за споделяне на пароли;
- задължителна периодична смяна на паролите (на 3 месеца за администратори; на 6 месеца за потребители).

Чл. 12. Всеки служител и ученик използва уникален потребителски профил. Използването на общи или групови профили е забранено.

Чл. 13. Лицата, които обработват лични данни, използват уникални пароли с висока сложност, които не се записват или съхраняват на достъпни места.

- Паролите трябва да са минимум 8 символа за потребителските профили и 12 символа за администраторските профили.
- Да съдържат комбинация от букви, цифри и символи.
- Смяна на паролата: поне на 90 дни за администратори и поне на 180 дни за потребители.
- Забрана за повторно използване на стари пароли.



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

- При възможност – използване на многофакторно удостоверяване (MFA).

Чл. 14. Предоставянето и отнемането на достъп се извършва по определен ред, съобразен с длъжността и нуждите на служителя.

- Предоставените потребителски имена и нива на достъп се записват в Регистър за достъп – Приложение 4.
- Всеки служител подписва Декларация за спазване на правилата за информационна сигурност – Приложение 5.
- Учениците преминават инструктаж за правилата при работа в компютърните кабинети – Приложение 3.

Чл. 15. Носители на лични данни и чувствителна информация се съхраняват в заключени помещения или шкафове с контролиран достъп.

Чл. 16. Забранява се:

- изнасяне на бази данни извън служебните помещения без разрешение;
- използване на данни извън служебните задължения;
- предоставяне на данни на трети лица без заявена услуга и разрешение.

Чл. 17. Унищожаването на остарели или ненужни носители се извършва чрез сигурно физическо унищожаване (шредиране или друго), като процесът се документира.



СРЕДНО УЧИЛИЩЕ "СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ" АСЕНОВГРАД

ул. "Княгиня Евдокия" □41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.sus5km.com>

РАЗДЕЛ IV. ПРАВИЛА ЗА РАБОТНОТО МЯСТО И ОТГОВОРНОСТИ НА ПОТРЕБИТЕЛИТЕ

Чл. 18. Работното място трябва да бъде организирано така, че да се предотврати нерегламентиран достъп до екрана, хартиени документи, носители и служебна информация. Мониторите следва да бъдат разположени така, че съдържанието да не може да бъде наблюдавано от външни лица.

Чл. 19. Потребителите са длъжни:

- да заключват работната станция при временно отсъствие;
- да изключват компютрите в края на работния ден;
- да не оставят служебни документи и носители на бюрото без надзор;
- да докладват при забелязани нередности или инциденти.

Чл. 20. При работа с данни, съдържащи лична или чувствителна информация, тя се разглежда и обработва само на определени за целта устройства.

Чл. 21. Забранява се заобикалянето на технически мерки за сигурност, включително:

- защитни стени;
- антивирусни решения;
- филтри за интернет достъп;
- политики за контрол на достъпа;
- ограничения за системни настройки.

Чл. 22. При напускане на работното място за период по-дълъг от 10 минути потребителят трябва да заключи устройството (Win + L).

Чл. 23. Всички служители са длъжни да спазват Политиката за използване на интернет, утвърдена в училището.

Чл. 24. Забранява се използването на лични устройства за работа с чувствителна училищна информация без разрешение (BYOD /Bring Your Own Device/ политика).



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

Чл. 25. Забранява се отстраняването, преместването или манипулирането на мрежово оборудване (рутери, суичове, Wi-Fi точки, кабели).

Чл. 26. Повреда на хардуер или софтуер се докладва незабавно на системния администратор.

Чл. 27. Потребителите са длъжни да спазват всички правила, свързани със защита на личните данни (GDPR).

Чл. 28. Забранява се записването на входни данни (потребителско име, парола) на видими места. При съмнение за компрометирана парола – тя се сменя незабавно.

Чл. 29. При установяване на нарушение учебното заведение предприема съответните дисциплинарни мерки.

Чл. 30. Потребителите преминават инструктаж за информационна сигурност поне веднъж годишно – съгласно Приложение 3.



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. “Княгиня Евдокия” □41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.suskm.com>

РАЗДЕЛ V. МРЕЖОВА СИГУРНОСТ И ПОЛИТИКИ ЗА ИНТЕРНЕТ

1. Мрежова структура и контрол

Чл. 31. В училището се прилага мрежова сегментация, включваща минимум:

- Административна мрежа – за деловодство, администрация, счетоводство и служебни системи;
- Учителска мрежа – за служебни устройства на педагогическия персонал;
- Ученическа мрежа/обучителна зона – за компютърни кабинети и BYOD при необходимост;
- Гост мрежа – само при нужда, с ограничен достъп.

Чл. 32. Административната мрежа (обслужваща административните помещения) и Ученическата мрежа/Обучителната зона (обслужваща компютърните кабинети) се осигуряват от отделни доставчици на интернет свързаност и функционират като самостоятелни логически мрежи, различни от основните мрежи.

Чл. 33. Забранява се свързването на потребителски устройства между отделни LAN мрежи чрез Wi-Fi мостове, точки за достъп, донесени от потребители, или други опити за заобикаляне на сегментацията.

Чл. 34. В училището са инсталирани камери за видеонаблюдение в коридорите и в някои кабинети. Те се използват единствено за целите на сигурността и контрола на достъпа, като достъп до записите имат само упълномощени лица.

Чл. 35. Всички ключови мрежови устройства се защитават чрез:

- силни уникални пароли;
- ограничен физически достъп;
- редовни актуализации на фърмуер.

2. Защитна стена и интернет филтриране

Чл. 36. Целият интернет трафик преминава през защитна стена (firewall), която осигурява:

- филтриране по протоколи и адреси;



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

- ограничение за нежелано съдържание;
- защита от злонамерен трафик.

Чл. 37. Достъпът до административните системи от външни мрежи се осъществява само чрез защитени канали, при наличие на необходимост и с разрешение от директора.

3. Wi-Fi сигурност

Чл. 38. Безжичните мрежи се конфигурират с WPA2-Enterprise или WPA3 (ако оборудването позволява), с отделни SSID за различни групи потребители.

Чл. 39. Забранява се споделяне на паролата с външни лица.

Чл. 40. Периодична смяна на пароите на Wi-Fi се извършва най-малко на всеки 6 месеца.

4. Антивирусни и защитни решения

Чл. 41. Всички служебни устройства използват антивирусен софтуер с активна защита в реално време.

Чл. 42. Забранява се деактивиране на защитата или заобикаляне на настройките.

Чл. 43. Актуализация на дефинициите за вируси се извършва автоматично.

5. Обработка и логване на събития

Чл. 44. Системите поддържат логове за достъп до системи, промяна на права, опити за пробив и системни грешки.

Чл. 45. Логовете се съхраняват минимум 6 месеца, а за критични системи – 1 година.

Чл. 46. До логовете имат достъп само оторизирани администратори.



СРЕДНО УЧИЛИЩЕ "СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ" АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

РАЗДЕЛ VI. ПЛАН ЗА РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ

Чл. 47. Инцидент е всяко събитие, което застрашава сигурността на данните или системите.

Примери за инциденти:

- вируси и злонамерен софтуер;
- нерегламентиран достъп до системи или мрежи;
- пробив в защита или компрометирана парола;
- загуба или кражба на устройство;
- неправомерно публикуване на данни;
- отказ на критична услуга (електронен дневник, счетоводна система).

Чл. 48. При установяване на инцидент потребителят незабавно уведомява:

- системния администратор;
- ЗД АСД;
- директора при сериозни инциденти.
- Докладването се извършва в рамките на **24 часа** чрез устно уведомяване и попълване на **Формуляр за докладване на инцидент – Приложение 6**.

Чл. 49. Системният администратор предприема следните действия:

- изолиране на засегнатото устройство или мрежов сегмент;
- проверка за разпространение на проблема;
- анализ на логове и събития;
- отстраняване на проблема и възстановяване на нормалната работа;
- изготвяне на доклад до директора.

Чл. 50. При инцидент, свързан с лични данни, училището уведомява Регионалния инспекторат и/или Комисията за защита на личните данни (КЗЛД), ако е необходимо, в срок до **72 часа** от установяване на нарушението.



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

Чл. 51. Всички инциденти се вписват в Регистър на инцидентите – част от Приложение 6, който се съхранява от системния администратор и се преглежда периодично от директора.



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

Тел/факс: 0331/64787
<http://www.susskm.com>

РАЗДЕЛ VII. АРХИВИРАНЕ И ВЪЗСТАНОВЯВАНЕ

Чл. 52. Критични системи на училището (администрация, деловодство, електронен дневник, счетоводство) подлежат на:

- ежедневен автоматичен архив;
- седмичен външен архив на отделен носител или криптиран облак.

Чл. 53. Архивите се съхраняват на защитени носители или в криптирани облачни услуги, като достъп до тях има само системният администратор и директорът.

Чл. 53а. Архивирането на електронния дневник („Школо“), административните и счетоводните системи (вкл. НЕИСПУО на МОН) се извършва от външните доставчици на услугата, съгласно сключените договори и абонаменти. Училището осигурява контрол върху изпълнението чрез системния администратор и директора, които следят за наличието на договор и редовно извършвано архивиране.

Чл. 54. Отговорността за създаването, съхранението и проверката на архивите се носи от системния администратор.

Чл. 55. Поне веднъж годишно се извършва тест за възстановяване на данните, като резултатите се документират в Приложение 7 – Чеклист за проверка на сигурността.

Чл. 56. При възникване на инцидент или загуба на данни, възстановяването се извършва по предварително утвърден план, като се използват най-новите налични архиви.



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. “Княгиня Евдокия” №41
email: info-1600116@edu.mon.bg

телефон/факс: 0331/64787
<http://www.susskm.com>

РАЗДЕЛ VIII. ОБУЧЕНИЕ И ПОВИШАВАНЕ НА КВАЛИФИКАЦИЯТА

Чл. 57. Всички служители преминават обучение по информационна сигурност минимум веднъж годишно. Обучението включва теми като:

- разпознаване на фишинг и социално инженерство;
- работа с лични данни съгласно GDPR;
- процедури при инциденти и докладване;
- добри практики за работа с пароли и устройства.

Чл. 58. Новоназначени служители преминават инструктаж по информационна сигурност при постъпване на работа, като подписват декларация за спазване на правилата – Приложение 5.

Чл. 59. Учениците преминават кратък инструктаж в началото на всяка учебна година относно правилата за работа в компютърните кабинети и училищната мрежа – Приложение 3.

Чл. 60. Учителите са длъжни да напомнят на учениците за правилата при работа в компютърните кабинети и да докладват при установени нарушения.

Чл. 61. При необходимост училището може да организира допълнителни обучения или семинари за служители и ученици, свързани с нови технологии, киберсигурност и защита на личните данни.



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" №41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

РАЗДЕЛ IX. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 62. Настоящите правила влизат в сила от датата на утвърждаването им със заповед на директора на СУ „Св. св. Кирил и Методий“ – Асеновград.

Чл. 63. За нарушения на правилата се налагат дисциплинарни мерки съгласно действащата нормативна база и вътрешния правилник на училището.

Чл. 64. Документът се актуализира ежегодно или при промяна в нормативната уредба.

Чл. 65. Ръководителите и служителите в СУ „Св. св. Кирил и Методий“ – Асеновград са длъжни да познават и спазват разпоредбите на тези правила.

Чл. 66. Контролът по спазване на правилата се осъществява от директора и ЗД АСД, които извършват периодични проверки и оценяват ефективността им.

Чл. 67. Настоящите вътрешни правила се разглеждат и оценяват периодично, като училището може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими за защитата на информацията.

Чл. 68. Правилата са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност (ПМС № 186 от 26.07.2019 г.) и влизат в сила от датата на утвърждаване със заповед на директора.



СРЕДНО УЧИЛИЩЕ "СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ" АСЕНОВГРАД

ул. "Княгиня Евдокия" □41
email: info-1600116@edu.mon.bg

телефакс: 0331/64787
<http://www.susskm.com>

РАЗДЕЛ X. ПРИЛОЖЕНИЯ

Приложение 1 – Регистър на техниката

- Списък на всички компютри, периферни устройства и мрежово оборудване в училището.
- Включва: инвентарен номер, местоположение, дата на придобиване, отговорно лице.

Приложение 2 – Регистър за поддръжка

- Документира ремонти, профилактика и подмяна на компоненти.
- Включва: дата, вид дейност, извършено лице/фирма, резултат.

Приложение 3 – Инструктаж за ученици

- Формуляр/лист за инструктаж на учениците при работа в компютърните кабинети и училищната мрежа.
- Учениците се запознават с правилата и подписват за информираност.

Приложение 4 – Регистър за достъп

- Списък на предоставените потребителски имена и нива на достъп.
- Води се от системния администратор.

Приложение 5 – Декларация за спазване на правилата

- Подписва се от всеки служител при постъпване.
- Потвърждава, че лицето е запознато с правилата за информационна сигурност и GDPR.

Приложение 6 – Формуляр за докладване на инцидент

- Попълва се при установен проблем (вирус, нерегламентиран достъп, загуба на устройство).
- Включва: дата, описание, засегнати системи, предприети действия, лице, което докладва.



СРЕДНО УЧИЛИЩЕ “СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ” АСЕНОВГРАД

ул. "Княгиня Евдокия" □41
email: info-1600116@edu.mon.bg

☎ тел/факс: 0331/64787
<http://www.susskm.com>

Приложение 7 – Чеклист за проверка на сигурността

- Списък с контролни точки за периодична проверка от системния администратор.
- Включва: актуализации, състояние на антивируса, архиви, смяна на пароли, Wi-Fi настройки.

ПРАВИЛА ЗА РАБОТА В КОМПЮТЪРНИ КАБИНЕТИ И БЕЗОПАСНОСТ В ИНТЕРНЕТ

УТВЪРДИЛ:
ДИРЕКТОР:
/М. КРАЕВА/



I. Общи положения

- Учениците удостоверяват с подпис, че са запознати с правилата в началото на учебната година.
- Родителите се информират на първата родителска среща и съдействат за спазването им.
- Спазват се здравно-хигиенните изисквания за работа с компютър (Наредба № 9 на Министерство на здравеопазването).
- Работата в мрежа и Интернет се извършва само под ръководството на учителя и съгласно правилата за онлайн безопасност.
- Кабинетите се ползват по предварително утвърден график.
- При пожар, земетресение или бедствие учениците се извеждат организирано от учителя.

II. Задължения на ученика

На учениците се забранява:

- Влизане в кабинет без учител или без проведен инструктаж.
- Внасяне на храни, напитки, остри и опасни предмети, както и всякакви течности – включително вода, сокове, коректори, лепила и други вещества, които могат да повредят техниката.
- Пипане и ремонтване на електрическата инсталация, кабели, табла, ключове, контакти.
- Ремонт, разместване или игра с компютри, монитори, периферия и мрежово оборудване.
- Премахване на гаранционни лепенки.
- Включване/изключване на компютри без разрешение на учителя.
- Работа с външни носители (флашки, дискове) без разрешение.
- Смяна на работно място без разрешение.
- Тичане, блъскане и игра с предмети в кабинета.
- Драскане или лепене на стикери по техника, мебели и стени.
- Работа с нерегламентирани програми, игри или сайтове.
- Посещаване на опасни онлайн страници, чатове с непознати, споделяне на лични данни.
- Извършването на кибертормоз чрез публикации, съобщения или материали в интернет и социалните мрежи.
- Публикуването в социалните мрежи на снимки или видеоклипове, които уронват авторитета на други лица или на училището.

Ученикът е длъжен:

- Да заеме определеното от учителя място.
- Да следва указанията на преподавателя.
- Да съобщи незабавно при липси, повреди или нередности.
- Да пази техниката и поддържа работното място чисто и подредено.
- Да напуска кабинета организирано само след разрешение.

III. Задължения на преподавателя

- Провежда инструктаж на ученици и родители за безопасна работа с компютърна техника.
- Осигурява подреждането на оборудването в кабинета по начин, който е удобен и безопасен за работа, като гарантира, че всеки ученик разполага с работно място.
- В началото на учебната година провежда инструктаж по безопасни условия на труд (БУТ) и противопожарна безопасност (ПО), като го регистрира в книгата за инструктаж.
- Провежда ежедневен инструктаж преди всяко учебно занятие за безопасна работа, като запознава учениците с възможните последствия при неспазване на правилата.
- Не възлага на учениците несвойствени за тях задачи.
- Спазва учебната програма и нормите за работа с компютър (времетраене, почивки).
- Провежда два последователни учебни часа само при осигурена междучасна почивка от 10–20 минути.
- Следи за опазването на техниката и води тетрадка-дневник за нейното състояние.
- При повреда незабавно уведомява отговорното лице.
- След приключване на часа проверява техниката, затваря прозорците и заключва кабинета.
- Последният учител за деня изключва цялата техника и след това спира електрозахранването на кабинета.

IV. Задължения на ръководителя на направление ИКТ

- Носи отговорност за компютърната техника в училището, като следи нейното движение и състояние.
- Запознава учениците с правилата за безопасно използване на дигиталните технологии, включително работа в интернет среда, и разяснява отговорното поведение в училищната мрежа и онлайн.
- Извършва периодичен преглед на училищната мрежа с цел откриване на възможни заплахи и рискове за сигурността на учениците при работа в интернет.
- Уведомява незабавно директора на училището при установяване на нарушения на правилата или при наличие на незаконно съдържание в мрежата.

V. Отговорност

- При нарушение учениците носят административна отговорност, а родителите материална.
- Повредено имущество се възстановява от виновния ученик/родител в срок до 7 дни.
- При неизяснен извършител щетата се възстановява от всички ползвали работното място.

VI. Правила за безопасен интернет

- Учениците не споделят лични данни, снимки, пароли или телефони онлайн.
- Забранява се чатене с непознати лица и отваряне на подозрителни линкове.
- Забранява се сваляне на програми и файлове без разрешение на учителя.
- Работи се само в образователни, разрешени и безопасни сайтове.
- При съмнително съдържание или онлайн опасност ученикът незабавно уведомява учителя.