

Утвърдил:
Йълдъз Реджеб
Директор



ПОЛИТИКА ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

РАЗДЕЛ I. ОСНОВНИ ПОЛОЖЕНИЯ

Чл.1 С настоящата политика се уреждат управлението, контрола и използването на информацията, публикувана в интернет пространството, информацията в мрежовата система и използването на компютърното оборудване в ДГ „Св. Св. Кирил и Методий“. Целта на тези правила е:

- да гарантира ефикасното използване на компютрите;
- да гарантира, че служителите ще използват предоставените им компютри и Интернет връзка в съответствие с изпълнението на служебните им задължения и само за тази цел;
- да предотврати възможно застрашаване целостта на информацията в мрежовата инфраструктура на ДГ „Св. Св. Кирил и Методий“

Чл.2. Всички компютри са свързани чрез мрежа и не се толерира никакво застрашаване на тази система.

Чл.3. Правилата важат за всички служители, работещи в ДГ „Св. Св. Кирил и Методий“ със служебни компютри.

РАЗДЕЛ II. ДОСТЪП И ПАРОЛИ

Чл.4. Достъпът до Интернет, електронната поща и компютърното оборудване, осигурени от и предоставени на ДГ „Св. Св. Кирил и Методий“ са само за служебно ползване. Използването им за лични цели е забранено.

Чл.5. Забранява се достъпа до компютърните файлове на други служители. Разрешение за това дава съответния потребител, при наличието на основателна причина / отсъствие на служител /

Чл.6. Паролите за достъп до служебните компютри и програмни продукти, се съхраняват от самите служители

Чл.7. Служителите не могат да отстъпват паролите си за достъп до системата на други служители, външни лица, роднини и приятели;

Чл.8. Всеки служител има лична парола и персонална идентификация, която не предоставя за използване от други лица и е достатъчно защитена

Чл.9. При съмнение за нарушение на сигурността на личните данни, лицето, което е установило несъответствието (случайно или неправомерно унищожаване на лични данни, загуба, промяна, неразрешено разкриване или нерегламентиран достъп), незабавно уведомява директора

РАЗДЕЛ III. РАБОТА С ПРОГРАМНИ ПРОДУКТИ

Чл.10. Не се позволява инсталирането на какъвто и да е нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за поправка или подобрения на горепосочените.

Чл.11. При съмнение за възникнал проблем при работа с програмен продукт , незабавно се уведомява експертът по Информационно осигуряване , съответните оторизирани фирми , разработили програмния продукт.

Чл.12. Използването на внесени отвън информационни носители(оптични дискове, дискети, флаш памети и др.), става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват;

Чл.13. Инсталирането на софтуерни програми, несъотнесими към пряката служебна работа е ЗАБРАНЕНО

РАЗДЕЛ III. ИЗПОЛЗВАНЕ НА ИНТЕРНЕТ И ЕЛЕКТРОННА ПОЩА

Чл.14. Достъпът до Интернет става чрез инсталирани на персоналните компютри браузър

Чл.15. Не се разрешава използването на Интернет връзката за гледане на видео или филми от служителите, което значително намаляват скоростта на връзката на другите служители.

Чл.16. Правилата за достъп на служителите до Интернет включват следните задължителни изисквания:

16.1. Не се толерира влизането в Интернет - сайтове с неизвестно съдържание;

16.2. Използването на чат - програми е единствено и само за служебна цел;

16.3. Не се разрешава инсталирането на други чат-програми, освен електронна поща;

16.4. Не се разрешава тегленето на файлове с неизвестно съдържание от Интернет.

16.5. Ползването (отварянето) на изтеглени файлове от Интернет пространството (сайтове, лични пощи, форуми, чат-програми и др.) във връзка с изпълнение на служебните задължения, става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, файловете се изтриват незабавно;

Чл.17.

17.1.Достъпът до електронна поща на ДГ „Св. Св. Кирил и Методий“-
cdg_glavinica@abv.bg се осъществява от директора и заместник-директори, Гл.
счетоводител, Техн. секретар, Касиер-домакин имат служебни електронни пощи.

17.2.Постъпилата информация по ел. поща , касаеща дейността на, гл. счетоводител,
технически секретар / писма, справки НАП, съобщение РМС -заплащане наем , фактури,
извлечения ЦКБ , информация за банкови преводи от ePay.bg , искания за справки и др.
/ се препраща към техните лични служебни имейли.

17.3.Съобщения , изпратени от ел. поща на ДГ – cdg_glavinica@abv.bg - са
законосъобразни и подлежат на изпълнение.

17.4.Всяко съобщение , което ЗД ,главен счетоводител ,технически секретар изпращат
в изпълнение на отговорности от техните служебни ел. адреси , е подписано от тях с
имена и длъжност .

17.5.При отсъствие на директора , в заповедта се конкретизира длъжностно лице , на
което е даден достъп до ел. поща на ДГ „Св. Св. Кирил и Методий“

Чл.18. Правилата за достъп и използването на електронната поща, включват следните
задължителни изисквания:

18.1.Служителите не трябва да отварят съобщения, получени от неизвестен получател
или неизвестна Интернет страница. Такива съобщения се изтриват незабавно;

18.2.Прикачените файлове към съобщенията, получени в служебните пощи ,не се отварят
при съмнение за вируси;

Чл.19. Служителите преместват важната информация от получените съобщения в
отделни файлове върху техните компютри.

РАЗДЕЛ IV. РАБОТА С КОПИР, ПРИНТЕР , СКЕНЕР

Чл.20. Не се допуска:

(1) Самостоятелни опити за поправка на принтерна, копирна и друга техника. При
сомнение за съществуващ проблем служителите следва да се обръщат към оторизирана
фирма

(2) Смяната на тонер-касети и отстраняването на заседнали листи се извършва на място,
само от обучени за това служители.

(3) Техниката се използва изключително и само за служебни цели;

РАЗДЕЛ V. АРХИВИРАНЕ И УНИЩОЖАВАНЕ (ИЗТРИВАНЕ) НА ЕЛЕКТРОННИ ДОКУМЕНТИ

Чл.21. Създадените файлове от служителите на персоналните им компютри, както
запазените файлове от съобщенията в електронните пощи, които вече не са необходими
с оглед изпълняването на служебните задължения, се изтриват периодично;

Чл.22. С цел недопускане на загуба на информация ,всяка важна информация се съхранява в диск "D " на компютъра , както и на преносима памет , която периодично се актуализира

РАЗДЕЛ VI ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

чл.23.Настоящата политика е разработена в съответствие с Постановление № 186 от 19 юли 2019 г. за приемане на Наредба за минималните изисквания за мрежова и информационна сигурност и подлежи на актуализиране при промяна на нормативната база.

чл.24.Настоящата политика се преразглежда редовно, но не по-рядко от веднъж годишно, и при необходимост се актуализира.