СРЕДНО УЧИЛИЩЕ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“ – БУРГАС

8010 Бургас, ж.к. „П. Р. Славейков” до бл.44, Директор: 056 860905;
Заместник-директори: тел./факс: 056 860847; Канцелария: 056 860906;
E ...

УТВЪРЖДАВАМ,
ДИРЕКТОР:
МАРТИН ИЛИЕВ

СРЕДНО УЧИЛИЩЕ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“ ОБЩИНА БУРГАС

ВЪТРЕШНИ ПРАВИЛА

НА СРЕДНО УЧИЛИЩЕ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“ - БУРГАС ЗА МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ СЪГЛАСНО РЕГЛАМЕНТ 2016/679

утвърдени със Заповед № РД-07-1249/ 22.06.2018 г.

на Директора на Средно училище „Епископ Константин Преславски“ – Бургас

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) **СРЕДНО УЧИЛИЩЕ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“ – БУРГАС**, е юридическо лице, със седалище и адрес на управление: гр. Бургас, к/с „Славейков“, до бл. 44, БУЛСТАТ: **000048600**

(2) Настоящите вътрешни правила уреждат условията и реда за водене на регистри по Закона за защита на личните данни (ЗЗЛД), както и организацията и реда за упражняване на контрол при обработването на лични данни от служителите на Средно училище „Епископ Константин Преславски“ – Бургас.

(3) По смисъла на настоящите правила и Закона за защита на личните данни обработване на личните данни е всяко действие или съвкупност от действия, които могат да се извършат по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване или предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.

(4) Обработване на личните данни в Средно училище „Епископ Константин Преславски“ – Бургас се състои и в осигуряване на достъпа до определена информация само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

Чл. 2. (1) Вътрешните правила се приемат с цел да регламентират:

1. създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;
2. видовете регистри, които се водят в образователната институция и тяхното описание.
3. необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).
4. правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната

отговорност при неизпълнение на тези задължения.

5. процедури за докладване, управляване и реагиране при инциденти.

(2) Вътрешните правила се утвърждават, допълват, изменят и отменят от Директора на Средно училище „Епископ Константин Преславски“ – Бургас и със срок на действие - постоянен.

Чл. 3. Настоящите вътрешни правила се прилагат за лични данни по смисъла на Закона за защита на личните данни и се издават на основание чл.13, ал.1 от Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на лични данни на Комисията за защита на личните данни.

Чл. 4. Средно училище „Епископ Константин Преславски“ – Бургас е администратор на лични данни по смисъла на чл.3, ал.1 от Закона за защита на личните данни.

Чл. 5. (1) Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) Личните данни се събират за конкретни, точно определени и законни цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

II. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 6. (1) Администраторът възлага обработването на личните данни на негови служители (обработващи). Обработването се възлага на повече от един обработващ данните, съобразно спецификата на изпълняваните от тях служебни функции и с цел разграничаване на конкретните им задължения.

(2) Обработващите лични данни, действат само по указание на администратора, освен ако в закон не е предвидено друго.

Чл. 7. (1) Личните данни в регистрите се набират от администратора на лични данни респективно - обработващият лични данни чрез устно интервю и/или на хартиен носител.

(2) За необходимостта от набирането на данните и целите, за които ще бъдат използвани, обработващият данните информира лицето, след което се предоставят на ресорния ръководител на хартиен носител. Ако намери за необходимо ресорният ръководител, съгласува решението си с длъжностните лица, упражняващи оперативен и цялостен контрол.

(3) За достоверността на предоставените копия от регистри, съдържащи лични данни, отговорност носи обработващият лични данни.

(4) Съхраняването на лични данни на хартиен носител се осъществява като данните се съхраняват: в папки в определени шкафове и не се изнасят от сградата на образователната институция, освен от обработващия лични данни, при служебна необходимост и на технически носител като на всеки 7 дни, обработващия лични данни ги архивира.

III. ФОРМИ НА ВОДЕНЕ НА РЕГИСТРИТЕ

Чл. 8. Форма на организация и съхраняване на личните данни на хартиен носител:

(1) Папките са разположени върху работните бюра и в офис шкафове в кабинетите на служителите, които се заключват. Правата и задълженията на служителите са регламентирани в длъжностните им характеристики. Предоставянето, промяната или прекратяването на оторизиран достъп до регистри се контролира от директора и от завеждащия административна служба.

(2) Местонахождение на картотечния шкаф - може да бъде поставен в помещение, предназначено за самостоятелна работа на обработващия лични данни или в общо помещение за работа с изпълняващи други дейности.

(3) Носител (форма) за предоставяне на данните от физическите лица - личните данни за всяко лице се набират в изпълнение на нормативно задължение (разпоредбите на закони, подзаконови нормативни актове, кодекси и други) чрез:

- устно интервю с лицето;

- хартиен носител - писмени документи (заявления) по текущи въпроси в процеса на работа, подадени от лицето;

- външни източници (съдебни, финансови, осигурителни, данъчни и др. институции в изпълнение на нормативни изисквания).

(4) Личните данни от лицата се подават до администратора на личните данни – Средно училище „Епископ Константин Преславски“ – Бургас, представляван от директора на образователната институция и длъжностното лице, определено за обработване на лични данни със заповед на директора на образователната институция.

(5) Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и изрично е регламентирана в Раздел I на настоящите Вътрешни правила.

Чл. 9. Форма на организация и съхраняване на личните данни от Средно училище „Епископ Константин Преславски“ – Бургас на технически носител:

(1) Личните данни се въвеждат на твърд диск на сървър от компютърната мрежа (в случай, че се обработват от повече от един служител) или на изолиран компютър (в случай, че се обработват само от един служител или от съответното работно място не може да бъде осигурен достъп до сървър). Компютърът е свързан в локалната мрежа, със защитен достъп до личните данни, с който може да работи само обработващият лични данни и мерки при средно ниво, съобразно изискванията на Наредба № 1 от 7.02.2007 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

(2) При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на администратора на лични данни. Данните се въвеждат в компютъра от хартиен носител.

(3) Достъп до файловете за обработка на лични данни имат само работещите с нея. Носители с лични данни могат да се разпространяват само ако данните са криптирани или ако е използван друг механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.

(4) Местонахождение на сървъра – съобразно изискванията на Вътрешни правила за информационните системи в Средно училище „Епископ Константин Преславски“ – Бургас местонахождение на компютрите - в изолирано помещение за самостоятелна работа на обработващия лични данни по регистъра, и в общо помещение с изпълняващи други дейности без право на достъп до него на останалите служители. Правото на достъп е регламентирано в специално изготвени декларации.

(5) Достъп до файловете за обработка на лични данни има само определено със заповед на директора лице обработващо лични данни чрез парола за отваряне на тези файлове, известна на него.

(6) Защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни електронни носители, както и чрез съхраняване на информацията на хартиен носител. Когато данните се намират на сървър, архивирането им се извършва от отговорен служител. Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър (обработващия лични данни).

IV. МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ

Чл. 10. (1) *Физическа защита* в училището се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни.

(2) Основните приложими *организационни мерки за физическа защита* в учебното заведение включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп.

Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на учебния и административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и на външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп, с оглед изпълнението на служебните им задължения.

Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

Организацията на физическия достъп до помещения, в които се обработват лични данни, е базирана на ограничен физически достъп (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

Като *зони с контролиран достъп* се определят всички помещения на територията на училището, в които се събират, обработват и съхраняват лични данни.

Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители са защитени по адекватен начин – в зони с контрол на достъпа.

(3) Основните приложими *технически мерки за физическа защита* в училището включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Чл. 11. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на политиката и ръководствата за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
5. съгласие за поемане на задължение за неразпространение на личните данни;

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае".

(4) Лицата могат да започнат да обработват лични данни след запознаване със:

1. нормативната уредба в областта на защитата на личните данни;
2. политиката и ръководствата за защита на личните данни;
3. опасностите за личните данни, обработвани от администратора.

Чл. 12. (1). Основните приложими *мерки за документална защита* на личните данни са:

1. *Определяне на регистрите, които ще се поддържат на хартиен носител*: на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на училището;

2. *Определяне на условията за обработване на лични данни*: личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на училището, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;

3. *Регламентиране на достъпа до регистрите*: достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае";

4. *Определяне на срокове за съхранение*: личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.

5. Процедури за унищожаване: Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на гимназията, се унищожават по подходящ и сигурен начин (напр. изгаряне,
нарязване, електронно изтриване и други подходящи за целта методи).

Чл. 13. (1) *Защитата на автоматизираните информационни системи и/или мрежи* в училището включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, оценени с ниско ниво на въздействие, включват:

1. *Идентификация* чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на училището. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразен с принципа „Необходимост да знае";

2. *Управление на регистрите*, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;

3. *Защитата от вируси*, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от учител по информационни технологии.

4. Политиката по *създаване и поддържане на резервни копия за възстановяване* регламентира предотвратяване загубата на информация, свързана с лични данни, която би затруднила нормалното функциониране на учебното заведение.

5. Основни електронни *носители на информация са*: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)

6. *Персоналната защита на данните* е част от цялостната охрана на училището.

7. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.

8. Данните, които вече не са необходими за целите на учебното заведение и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

Чл. 14. Служителите от Средно училище „Епископ Константин Преславски" – Бургас са длъжни да спазват и изпълняват настоящите вътрешни правила, в съответствие с длъжностните им характеристики.

Чл. 15. При обработване на личните данни служителят подписва декларация, че е запознат с изискванията на ЗЗДЛ, инструкцията относно механизма на обработване на лични данни и защитата им от незаконни форми на обработване, както и с настоящите вътрешни правила.

Чл. 16. (1) Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.

(2) Лични данни се предоставят служебно между структурните звена и служителите на образователната институция след обосновано искане, чрез докладна записка.

Чл. 17. (1) Всяко физическо лице има право на достъп до отнасящи се за него лични данни, съхранявани и обработвани в Средно училище „Епископ Константин Преславски" – Бургас.

(2) Правото на достъп се осъществява с писмено заявление/ или заявление по електронен път, подадено по реда на Закона за електронните документи и електронния подпис, до директора на образователната институция лично или от изрично упълномощено от него лице, чрез нотариално заверено пълномощно. Подаването на заявлението е безплатно.

(3) Заявлението съдържа:

- име, адрес и други данни за идентифициране на съответното физическо лице;
- описание на искането;
- предпочитана форма за предоставяне на информацията;
- подпис, дата на подаване на заявлението и адрес за кореспонденция;
- приложено пълномощно, когато заявлението се подава от упълномощено лице.

(4) Заявлението се завежда в деловодството на образователната институция.

(5) Достъп до данните на лицето се осигурява под формата на:

- устна справка;
- писмена справка;
- преглед на данните от самото лице или от упълномощеното такова;
- копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

(6) При подаване на заявление за осигуряване на достъп до лични данни, администраторът разглежда заявленията и разпорежда на обработващия лични данни да осигури искания достъп от лицето в предпочитаната от него форма.

(7) Срокът за разглеждане на заявлението и произнасянето по него е 14-дневен от деня на подаването му. Срокът може да бъде мотивирано удължен до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(8) Администраторът уведомява писмено заявителя за решението си – то може да бъде за предоставяне на достъп или отказ за достъп. Уведомяването става лично срещу подпис или по пощата с обратна разписка.

(9) Отказът на достъп до лични данни трябва да бъде мотивиран, а основанията за отказ са:

- когато данните не съществуват;
- когато данните не могат да бъдат предоставяни на определено правно основание.

(10) За отказ се счита и липсата на уведомление.

(11) Отказът за предоставяне на достъп до лични данни може да се обжалва от лицето в съда.

(12) Достъп до лични данни на лицата, съдържащи се на технически носител имат само определеният със заповед на директора - обработващ лични данни, който чрез парола има достъп до информацията и до съответния компютър.

(13) Освен на обработващият лични данни, правомерен е и достъпът на длъжностните лица, пряко ангажирани с оформянето и проверка законосъобразността на документите на лицата, отговарящи за съответната дейност, за която се водят регистри. Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

Чл. 18. (1) Лични данни се предоставят на трети лица само след получаване на писмено съгласие от лицето, за което се отнасят данните.

(2) При неполучаване на съгласие от лицето или при изричен отказ да се даде съгласие, данните не се предоставят.

(3) Не е необходимо съгласие на лицето в случаите, когато е задължен субект по закон.

(4) Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третото лице в 30-дневен срок от подаване на искането.

VI.ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЯНИЕ И РЕАКЦИЯ ПРИ ИНЦИДЕНТИ

Чл. 19. (1) При възникване и установяване на инцидент незабавно се докладва на лицето, отговорно за защита на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.

(3) След анализ от директора на образователната институция в дневника се записват последствията от инцидента и мерките, които са предприети за отстраняването им.

(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(5) В случаите на компрометирането на парола тя се подменя с нова, като събитието се отразява в дневника за инциденти.

VII. ВИДОВЕ РЕГИСТРИ, КОИТО СЕ ВОДЯТ В СРЕДНО УЧИЛИЩЕ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“ – БУРГАС

Видове регистри	Видове лични данни	Отговорни лица
Регистър „Персонал“ – щатен и извънщатен: - щатните работници и служители в Средно училище „Епископ Константин Преславски“ – Бургас, назначени по трудово право-отношение; - лицата, наети по граждански договори.	**физическа идентичност** – трите имена, ЕГН, постоянен адрес, телефони, месторождение, паспортни данни; **образование** – вид на образованието, специалност, място на придобиване на образованието, номер на диплома и дата на издаване, степени, звания и други; **трудова дейност** – трудов стаж в определена професия, стопански сектори, в които лицето е работило, трудово възнаграждение и други.	Директор; Заместник-директор по учебната дейност
Регистър „Ученици“: - **обучаваните ученици**, в различни форми на обучение – дневна или самостоятелна; - **родителите/настойниците** на обучаваните ученици.	**физическа идентичност** – трите имена, ЕГН, постоянен адрес, телефони, месторождение, паспортни или други данни; - данните се получават и съхраняват на хартиен носител в архива на образователната институция и на магнитен/електронен носител.	Заместник-директор по учебната дейност; Технически организатор; Класни ръководители; Други педагогически специалисти.
Регистър „Видеонаблюдение“: **- обучаваните ученици** в Средно училище „Епископ Константин Преславски“ – Бургас; - **родителите/настойниците** на обучаваните ученици; **- външни за образователната институция лица**	Запис чрез собствени технически средства за видеонаблюдение, за наличието на които са поставени информационни табели на видни места в училището, без да се уточнява тяхното местоположение. Записите от видеонаблюдението се съхраняват за срок от 24 часа. Записите съдържат "лични данни" или "лична информация" по смисъла на чл. 2, ал.1 от Закона за защита на личните данни, способна да разкрие физическата идентичност на лицето, което е записано.	Директор
Регистър „Доставчици“ – данни на лица, участващи в процеса на осъществяваната финансовата и друга дейност на училището.	**физическа идентичност –** наименование, БУЛСТАТ, седалище и банкова сметка	Директор Счетоводител
Регистър „Дипломи за завършено средно образование“	**физическа идентичност** – трите имена, ЕГН, месторождение.	Главен учител по информатика и информационни технологии

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

По смисъла на настоящите Вътрешни правила:

§1. „Администратор на лични данни” е Средно училище „Епископ Константин Преславски“ - Бургас, представлявано от директора на образователната институция.

§2. „Обработващ лични данни” са длъжностни лица от образователната институция, определени със заповед от директора на Средно училище „Епископ Константин Преславски“ – Бургас.

§3. Вътрешните правила влизат в сила от деня на тяхното утвърждаване.

§4. Настоящите Вътрешни правила за минимално ниво на технически и организационни мерки и за допустимия вид защита на лични данни, са приети и утвърдени на 22.06.2018 г. от директора на Средно училище „Епископ Константин Преславски“ - Бургас, на основание чл.23, ал.4 от ЗЗЛД, във връзка с чл.13, ал.1 от Наредба №1 за минималното ниво на технически и организационни мерки и допустимия вид защита на лични данни на Комисията за защита на личните данни.