ОУ „СВ. СВ. КИРИЛ И МЕТОДИЙ“ – ГР. ХАСКОВО
ул. „Страшимир“ №37, e-mail:kiril_imetodiy@abv.bg, тел. 038 / 66 82 88; 66 68 98

IVANKA ATANASOVA STOYANOVA
Digitally signed by IVANKA ATANASOVA STOYANOVA

УТВЪРЖДАВАМ:.....

ИВАНКА СТОЯНОВА

Директор на ОУ „Св. св. Кирил и Методий

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ОУ „СВ. СВ. КИРИЛ И МЕТОДИЙ“ ГР. ХАСКОВО

Настоящите вътрешни правила се издават от директора на училището на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД), утвърдени със Заповед № РД-14-81/18.10.2022 г.

Раздел I.
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) ОУ „Св. св. Кирил и Методий“ е юридическо лице със седалище гр. Хасково, РепубликаБългария, с основен предмет на дейност образование и образователни услуги.

(2) Училището обработва лични данни във връзка със своята дейност (образователна, възпитаваща, социализираща) и сама определя целите и средствата за обработването им.

Чл. 2. (1) Настоящите вътрешни правила уреждат организацията на обработване и защитата на лични данни на педагогическите специалисти, служителите, обучаемите (ученици), посетителите, както и на други физически лица, свързани с осъществяването на дейността на училището.

(2) Целта на настоящите вътрешни правила е установяването на ясни правила при събиране, организиране, съхраняване и разгласяване на лични данни от водените от ОУ „Св. св. Кирил и Методий“ регистри, за да се гарантира неприкосновеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентира правото на достъп до събираните и обработвани такива данни.

(3) Вътрешните правила се приемат с цел да регламентират:

- 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;

- 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).

- 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.

(4) Вътрешните правила се утвърждават, допълват, изменят и отменят от Директора на ОУ „Св. св. Кирил и Методий“ **Чл. 3.** Настоящите вътрешни правила се прилагат за лични данни по смисъла на Законаза защита на личните данни в Република България и Регламент (ЕС) 2016/679.

Чл. 4. (1) ОУ „Св. св. Кирил и Методий“ е администратор на лични данни по смисъла на чл. 4, пар. 7 от Регламент (ЕС) 2016/679.

(2) Според чл. 4, пар. 1 на Регламент (ЕС) 2016/679 „субект на лични данни“ е: идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.

Чл. 5. (1) Според чл. 4, пар. 1 на Регламент (ЕС) 2016/679 „лични данни“ са: всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) Според чл. 4, пар. 2 на Регламент (ЕС) 2016/679 „обработване“ е: всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване

(3) Личните данни се събират и обработват:

за изпълнение на правомощията и присъщата дейност на училището, предоставени чрез Закона и училищното и предучилищно образование и законодателството на Република

България и ЕС;
-въз основа на законови задължения, възложени чрез законодателството на Република България и ЕС /закони, наредби, инструкции, правилници, регламенти и др./;
- при сключване на договори или подготовка за тяхното сключване;
- за защита на жизненоважни интереси на субекта на данните или на друго физическо лице;
- при липса на някое от горепосочените основания – единствено след съгласие на субекта на лични данни, дадено чрез подписана декларация за съгласие по образец. *(Приложение № 1);*
- освен това когато обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете;

(4) Личните данни се обработват при спазване на следните принципи, въведени чрез Регламент 2016/679 г.:

1. Законосъобразност, добросъвестност и прозрачност - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

2. Ограничение на целите – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

3. Свеждане на данните до минимум – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;

4. Точност – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;

5. Ограничение на съхранението – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;

6. Цялостност и поверителност – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7. Отчетност – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

(5) Събирането на лични данни трябва да бъде в рамките на необходимото. Информацията се събира по законен и обективен начин; личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели; личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват; личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

Чл. 6. Училището организира и предприема мерки, за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване. Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. (1) ОУ „Св. св. Кирил и Методий“ прилага адекватна защита на личните данни, съобразенас нивото на нейното въздействие.

(2) Тя включва:

1. Физическа защита.
2. Персонална защита.
3. Документална защита.
4. Защита на автоматизирани информационни системи и/или мрежи.

Чл. 8. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по

начин, несъвместим с тези цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на училището и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на училището се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразено с посочените мерки за защита и нивото на въздействие на съответния регистър.

Чл. 9. За всяка дейност по събиране на лични данни се поддържа регистър на дейностите в *(Приложение № 3)* към настоящите Вътрешни правила, където е посочено кой, за какви цели и на какво основание обработва личните данни.

Чл. 10. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица.

(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на Директора на училището.

(3) Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции.

(4) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Чл. 11. (1) Документите и преписките, по които работата е приключила, се архивират.

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.

(3) Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Закона за Националния архивен фонд.

(4) Документите на електронен носител се съхраняват на специализирани компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и възможността и за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият/операторът/ на лични данни и оторизираните длъжностни лица.

(5) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани със заповед лица.

Чл. 12. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Чл. 13. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, служителят, констатирал това нарушение, докладва писмено за този инцидент на прекия си ръководител, който от своя страна е длъжен, своевременно да информира училищното ръководство.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

(3) Училищното ръководство трябва да уведоми Длъжностното лице по защита на личните данни и Комисията за защита на личните данни до 72 часа от узнаването за неправомерния достъп.

Чл. 14. При повишаване на нивото на чувствителност на информацията, произтичащо от

изменение в нейния вид или в рисковете при обработването й, училището може да определи друго ниво на защита за регистъра.

Чл. 15. (1) След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от училището регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни съобразно изискванията на Закона за защита на личните данни (чл. 25). При промени в структурата на училището, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.

(2) В случаите, когато се налага унищожаване на носител на лични данни, училището прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване данните и злоупотреба с тях. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване с шредер.

(3) Унищожаването се осъществява от служителя, отговорен за архива на училището-ЗАС.

Чл. 16. (1) Достъпът до данните от регистъра и разкриването на личните данни се осъществява при условията и по реда на Закона за защита на личните данни и Регламент 2016/679 от:

- физическите лица, за които се отнасят данните;
- трето лице, ако е предвидено в нормативен акт;
- обработващия личните данни.

(2) Достъп до лични данни може да бъде предоставен под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.

(3) Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

(4) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление*(Приложение № 2),* респ. искане за достъп до информация, и след тяхното легитимиране.

(5) Заявлението съдържа:

1. име, адрес и други необходими данни за идентифициране на съответното физическо лице;
2. описание на искането;
3. предпочитана форма за предоставяне на достъпа до личните данни;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(6) Директорът разглежда заявлението за достъп и се произнася по него в 14-дневен срок.

(7) Директорът взема решение за предоставянето на пълен или частичен достъп на заявителя или мотивира отказ за предоставяне на достъп.

(8) Директорът писмено уведомява заявителя за решението си. Уведомяването е лично срещу подпис или по пощата с обратна разписка.

Раздел II.
МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 17. (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 училището 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 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. 18. (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. съгласие за поемане на задължение за неразпространение на личните данни; изразено в декларация по образец. *(Приложение 4).*

(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. 19. (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 училището, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи).

Чл. 20. (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 упълномощено лице.
4. Политиката по *създаване и поддържане на резервни копия за възстановяване* има за цел предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на училището.
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 училището и чиито срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване с шредер, постоянно заличаване от електронните средства).

Чл. 21. (1) Компютърен достъп към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез парола.

(2) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

Чл. 22. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето й на сервизната организация се извършва, по възможност, без устройствата, на които се съхраняват лични данни.

Чл. 23. (1) В училището се използва единствено софтуер с уредени авторски права.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 24. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

Раздел III.
ПОДДЪРЖАНИ РЕГИСТРИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 25. Поддържаните регистри в училището са:

1. Човешки ресурси
2. Ученици
3. Родители
4. Проекти
5. Видеонаблюдение
6. Счетоводство и финансова отчетност
7. Контрагенти и доставчици
8. Архив

Чл. 26. (1) Всички регистри са подробно описани в Приложение № 3 към правилата, което представлява Регистър на дейностите. В него е посочено кой работи с данните от всеки един регистър и какви мерки за защитата им се предприемат.

(2) Всяка година Директорът издава заповед, с която определя кой да отговаря за всеки отделен регистър.

Чл.27. За всеки регистър се оценява рискът по следния начин:

(1) Ниско ниво на риска – когато загубата или неправомерното обработване на личните данни от конкретен регистър не биха имали значителни последствия, застрашаващи живота на физическо лице или кражба на самоличността му.

(2) Средно ниво на риска - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, довеждащи до кражба на самоличност на физическо лице.

(3) Високо ниво на риск - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, довеждащи до кражба на самоличност на група от физически лица.

(4) Изключително високо ниво на риск - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, застрашаващи живота на физическо лице.

Чл. 28. При „изключително високо ниво на риск“, констатирано при условията на предходния член, се извършва „Оценка на въздействието“ спрямо критериите, залегнали в Регламент (ЕС) 2016/679.

Раздел IV.
ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, РАБОТЕЩИ С ЛИЧНИ ДАННИ

Чл. 29. (1) Длъжностното лице по защита на данните е длъжно:

а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Общия регламент за защита на данните и на други разпоредби за защитата на данни на равнище Съюз или национално законодателство;

б) да наблюдава спазването на Общия регламент и на други разпоредби за защитата на данни на равнище Съюз или национално законодателство и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни;

в) да участва в повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

г) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;

д) надлежно да отчита рисковете, свързани с операциите по обработване, и да се съобразява с естеството, обхвата, контекста и целите на обработването;

е) да участва в заседания на ръководството, когато се обсъждат въпроси от областта на защитата на личните данни;

ж) да дава становище/съвет/мнение по всички въпроси, свързани със защитата на личните данни, да консултира администратора или обработващия лични данни;

з) да си сътрудничи с надзорния орган;

и) да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, и по целесъобразност да се консултира по всякакви други въпроси с надзорния орган;

(2) ДЛЗД има право:

а) да събира информация за определяне на дейностите по обработване;

б) да анализира и проверява изпълнението на дейностите по обработване;

в) да информира, съветва и отправя препоръки към администратора или обработващия лични данни;

д) да получава информация и необходимото съдействие от страна на ръководните органи в предприятието, от администратора/обработващия лични данни, от всички релевантни отдели и вътрешни структури, имащи отношение към операциите по обработване на лични данни.

(3) При изпълнение на своите задачи ДЛЗД действа напълно независимо и свободно от указанията на АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

Чл. 30. Служителите на училището са длъжни:

1. да обработват лични данни законосъобразно, добросъвестно и прозрачно;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. да актуализират регистрите на личните данни (при необходимост);
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
6. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си;
7. незабавно да уведомяват администратора на лични данни в случай, че установят изтичане на лични данни, независимо дали при извършване на своята работа или при друго лице, което обработва лични данни.

Чл. 31. (1) За неспазването на разпоредбите на Настоящите вътрешни правила служителите носят административна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни

са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

Раздел V.
ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Всички педагогически специалисти и служители в ОУ „Св. св. Кирил и Методий“ са длъжни срещу подпис да се запознаят с настоящите вътрешните правила за защита на личните данни ида ги спазват.

§ 2. Вътрешните правила се издават на основание чл. 23, ал. 4 от Закона за защита на личните данни и Регламент (ЕС) 2016/679.

§ 3. За всички неуредени в настоящите вътрешни правила въпроси са приложими разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни и действащото приложимо законодателство на Република България.

§ 4. Настоящите вътрешни правила отменят действието на съществуващата до сега Инструкция за защита на личните данни.

§ 5. Вътрешните правила се утвърждават със Заповед на Директора на ОУ „Св. св. Кирил и Методий“

Приложение 1.

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ

Долуподписаният/ата……
…….ЕГН: ……

ДЕКЛАРИРАМ:

Съгласен/а съм ……...
да обработва личните ми данни, съгласно изискванията на Регламент 2016/679/ЕС и Закона за защита на личните данни.

Запознат/а съм с:

- целта и средствата на обработка на личните данни;
- доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;
- правото ми на достъп и на коригиране на събраните данни;
- правото да оттегля съгласието си;
- получателите или категориите получатели, на които могат да бъдат разкрити данните.
- правото ми на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България.

Декларирам, че ще уведомявам администратора на лични данни за всяка промяна в личните ми данни.

Декларирам, че давам своето съгласие за обработване на лични данни свободно, съгласно волята си, и гарантирам верността на посочените данни:……

Дата: …… ДЕКЛАРАТОР:……

гр./с……..

Приложение 2.

До Директора на
ОУ „Св. св. Кирил и Методий“ – Хасково

ЗАЯВЛЕНИЕ
за предоставяне на лични данни

От…… с ЕГН ……

Пълномощник…… с ЕГН ……

Пълномощно №..... ,от .....(нотариално заверено, приложено към заявлението)

Относно: Предоставяне на лични данни .....
(описание на искането)

Уважаема г-жо Директор,

Във връзка с и на основание чл. 29, ал.1 от Закона за защита на личните данни (ЗЗЛД) с настоящото заявление се обръщам към Вас с оглед получаване на лични данни относно:

1 .....

2 .....

3 .....

Предпочитам формата на предоставената информация да бъде във вид на.....
(електронен вариант или на хартиен носител, електронна поща и др.)

Адрес за кореспонденция :

гр..... , ул. “ .....” №....., бл.,вх...., ет., ап ..... , тел.

Получател: .....
(име, презиме, фамилия)

Дата: С уважение:

Получено от:..... на..... г.

Приложе ние 3.

РЕГИСТЪР

1. Името и координатите за връзка на
- администратора;
- на представителя на администратора;
- на обработващия лични данни;
- на длъжностното лице по защита на данните.
2. Описание на регистъра.
3. Цели на обработването.
4. Наименование и данни за контакти на всички съвместни администратори— когато това е приложимо.
5. Субекти на лични данни.
6. Законово основание.
7. Категории (видове) лични данни, които се събират.
8. Категории получатели на лични данни.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава.
10.Гаранции за извънредни прехвърляния на лични данни към трети държави или международни организации (ако е приложимо).
11. График със срокове на съхранение.
12. Общо описание на техническите и организационни мерки за сигурност.
13. Основание за законосъобразност.
14. Основание за обработка на специални категории лични данни (ако е приложимо).
15. Източник на личните данни (ако е приложимо).
16. Местоположение (локация) на личните данни.
17. Има ли нарушение на сигурност на личните данни?
18. Връзка към документацията за нарушение на сигурността на лични данни.

Приложение 4.

ДЕКЛАРАЦИЯ
за неразпространение на лични данни

Подписаният/та *(име, презиме и фамилия)*
.....
На длъжност *(по длъжностна характеристика)*
…….....
.....

Д Е К Л А Р И Р А М, ЧЕ :

1. Няма да разпространявам информация за личните данни на трети лица, станали ми известни при изпълнение на служебните ми задължения и няма да ги използвам за други цели, освен за прякото изпълнение на служебните ми задължения.
2. Запознат/а/ съм със законодателството за защита на личните данни.
3. Нося отговорност за опазване на документите, съдържащи лични данни.
4. Запознат/а/ съм, че при разгласяване, предоставяне, публикуване, използване или разпространяване по друг начин на факти и обстоятелства, представляващи лични данни, нося административно-наказателна отговорност по Закона за защита на личните данни, дисциплинарна отговорност по Кодекса на труда, а в предвидените случаи и наказателна отговорност, ако деянието съставлява състав на престъпление по Наказателния кодекс.

Дата: …… ДЕКЛАРАТОР:…….....
(подпис)

гр……..

Приложение 5.

ДЕКЛАРАЦИЯ

Администратор на лични данни:.....

/име на училището/

Субект на лични данни:.....

/име, презиме, фамилия на ученика/

Относно следните лични данни: ……. /и всички други данни, необходими за попълване на документацията, получени от Вас при записването на ученика в училище/.

В качеството си на администратор на лични данни и изпълнявайки задълженията си съгласно Общия регламент за защита на данните декларирам, че ще използвам Вашите лични данни и личните данни на детето Ви, описани по-горе, за следната цел:

1. …….

Декларирам, че личните Ви данни ще бъдат третирани като строго поверителни и няма да бъдат споделяни.

Ще съхранявам Вашите лични данни не повече от предвидените в закона срокове: ……..,
като данните ще бъдат съхранявани по следния начин: всички документи, съдържащи лични данни, се съхраняват при необходимите технически и организационни мерки за защита.

Вашите права във връзка с настоящото събиране и обработване на личните Ви данни и личните данни на детето Ви са следните:

- имате право да поискате копие от Вашите лични данни и право на достъп по всяко време до личните си данни;
- имате право да прехвърлите личните си данни на друг администратор на лични данни, без да бъдете възпрепятствани от наша страна при налична такава законова възможност;
- имате право да поискате да коригирам без ненужно забавяне неточните Ви лични данни, както и данните, които не са вече актуални. За целите на коригиране или допълване на личните Ви данни трябва да подадете отделна декларация, в която да посочите актуални лични данни;
- имате право да поискате от администратора личните Ви данни да бъдат изтрити без ненужно забавяне при наличието на някое от следните основания: личните данни повече не са необходими за целите, за които са били събрани; когато сте оттеглил своето съгласие; когато сте възразил срещу обработването, когато обработването е незаконосъобразно; когато личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на ЕС или правото на държава членка, което се прилага спрямо администратора; когато личните данни са били събрани във връзка с предлагането на услуги на информационното общество.
- Администраторът може да откаже да заличи личните данни по следните причини:

1. упражняване на правото на свобода на изразяването и правото на информация;
2. за спазване на правно задължение от администратора или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратора;
3. по причини от обществен интерес и в областта на общественото здраве;
4. за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото съществува вероятност заличаването да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или за установяването, упражняването или защитата на правни претенции.

- имате право да поискате администратора на личните Ви данни, да ограничи обработването на личните Ви данни, като в този случай данните ще бъдат само съхранявани, но не и обработвани. Ако администраторът откаже да ограничи личните Ви данни, той следва да направи това само изрично и в писмен вид, като се мотивира за законосъобразната причина за този отказ.
- имате право да оттеглите Вашето съгласие за обработване на личните Ви данни по всяко

време с отделна молба, депозирана пред администратора в случаите, когато обработването се осъществява въз основа на дадено от Вас съгласие.
- имате право на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България.
- при нужда Вашите лични данни ще бъдат използвани за нова цел, която не е обхваната от настоящото известие за защита на данните, ще Ви се предостави ново известие за защита на данните, когато и където е необходимо, ще изискаме Вашето предварително съгласие за новото обработване.
Данни за контакт на администратора:.....
/адрес на училището, телефон/
Данни за контакт на длъжностното лице по защита на личните данни: ……

Дата . . . . . Подпис: . . . . . .
/За администратора на ЛД – Директор/

Долуподписаният .....(субекта на данни или родител на субекта на данни), с подписването на този формуляр потвърждавам, че съм прочел това известие за защита на данните, като съм получил разяснение на зададените от мен въпроси във връзка с текста и съм съгласен/а.....(име на училището) да съхранява и обработва моите лични данни (и тези на детето ми) за посочените в декларацията цели.

Дата…….. Подпис:……..

Приложение№ 6

Съгласие на родител за обработване лични данни на деца за образователни цели

Долуподписаният..... давам своето съгласие на . . . . . лични данни на детето . . . . . на възраст . . . . . да бъде използвана/ни за . . . . . цел …….

Запознат съм, че личните данни ще се съхраняват по следния начин: . . . . . , според законовите изисквания за защита на данните.

Запознат/а съм с:

- целта и средствата на обработка на личните данни;
- доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;
- правото ми на достъп и на коригиране на събраните данни;
- правото да оттегля съгласието си;
- получателите или категориите получатели, на които могат да бъдат разкрити данните;
- правото ми на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България..

Декларирам, че ще уведомявам администратора на лични данни за всяка промяна в личните данни на детето.

Запознат съм, че личните данни ще бъдат обработвани от тук посочения администратор на лични данни, а именно: ..... (посочват се имената и контактите на администратора).

Запознат съм, че имам право да оттегля съгласието си за обработване на лични данни на детето частично или изцяло по всяко време, за което следва да уведомя администратора по следния начин:. . . . . и на следните контакти:. . . . . .

Запознат съм, че имам право на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България.

Декларирам, че давам своето съгласие за обработване на лични данни свободно, съгласно волята си, и гарантирам верността на посочените данни.

Дата: …… ДЕКЛАРАТОР:……

гр./с……..

Приложение№ 7

ЗАЯВЛЕНИЕ

До Директора на
ОУ „Св. св. Кирил и Методий“

Долуподписаният……..…… с ЕГН..... , относно личните ми данни, а именно……., за които съм дал съгласие да обработвате.

Желая да прекратите обработването им и „да бъда забравен“, като за целта ги изтриете.

Дата…… Подпис:……..

Получено от:..... на..... г.

Приложение№ 8

ВЪЗРАЖЕНИЕ

До Директора на
ОУ „Св. св. Кирил и Методий“

Долуподписаният……...…… с ЕГН ……

С настоящото възразявам срещу обработването на личните ми данни от . . . . . .
. . . . . поради следната причина:
……
……

Дата . . . . . Подпис . . . . . .

Получено от:..... на..... г.