СУ„СВЕТИ ПАИСИЙ ХИЛЕНДАРСКИ”

с. СКАЛИЦА, обл. ЯМБОЛ

п.к. 8645, ул. „Христо Ботев” № 24, тел. 047959053,

e-mail: uchilishte_skalitsa@abv.bg

Информацията е заличена на основание на чл.2 от ЗЗЛД

Утвърждавам:

Директор на СУ „Свети Паисий Хилендарски“

ВЪТРЕШНИ ПРАВИЛА

за мерките за защита на личните данни
в Средно училище „ Свети Паисий Хилендарски“, с. Скалица

I. Общи положения

Чл. 1. (1) СУ „ Свети Паисий Хилендарски“, наричано за по – кратко СУ или училището е юридическо лице със седалище с. Скалица, общ. Тунджа, Р България с основен предмет на дейност образование и образователни услуги.
(2) Училището обработва лични данни във връзка със своята дейност и само определя целите и средствата за обработването им.
Чл. 2. Настоящите вътрешни правила уреждат организацията на обработване и защитата на лични данни на преподавателите, служителите, обучаемите (ученици), доставчици, както и на други физически лица, свързани с осъществяването на нормалната дейност на училището.
Чл. 3. (1) „Обработване на лични данни“ означава 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.
(2) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.
Чл. 4.Училището е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679.
Чл. 5. (1) „Лични данни“ означава 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) „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

Чл. 6. (1) Като администратор на лични данни, при обработването на лични данни СУ с. Скалица спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

Чл. 7. (1) Принципите за защита на личните данни са:

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.

(2) Ако конкретната цел или цели, за които се обработват лични данни от СУ, не изискват или вече не изискват идентифициране на субекта на данните, СУ не е задължено да поддържа, да се сдобие или да обработи допълнителна информация за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент 2016/679.

Чл. 8. 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. 9.(1) СУ „Свети Паисий Хилендарски“ прилага адекватна защита на личните данни, съобразена с 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. 10. (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 гимназията и/или нормалното й 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 предвидените мерки за защита и нивото на въздействие на съответния регистър.

Чл. 11. Когато не е налице хипотезата на, физическите лица, чл. 6, пар. 1, б. „б“ – „ е“ от Регламент 2016/679 чиито лични данни се обработват, подписват декларация за съгласие по образец. (Приложение № 1).

Чл. 12. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица, както и обработващи лични данни, на които администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защита на данните.

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

(3) Работниците и 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 по отношение на съответните работници и служители.

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

Чл. 13. (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 пожарогасители 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 ѝ 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 лица.

Чл. 14. (1). С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

(2) Служителите преминават задължителен инструктаж за запознаване с правилата за Противопожарна безопасност най-малко веднъж годишно. За проведения инструктаж се съставя Протокол по образец, съгласно ***Приложение № 2***.

Чл. 15. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на директора на училището, който от своя страна е длъжен, своевременно да информира Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

(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.

Чл. 16. (1) 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. 17.(1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от СУ регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, СУ прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(3) Унищожаване се осъществява от служителя, отговорен за архива на училището и след уведомяване на Длъжностното лице по защита на данните

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал. 3, съгласно образец, представляващ ***Приложение № 3***.

Чл. 18. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление лично или чрез нотариално заверено пълномощно (Приложение № 3), респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, училището съобщава в 14-дневен срок от подаване на заявлението, респ. искането.

(3) Срокът по ал. 2 може да бъде удължен от администратора 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.

(4) Информацията може да бъде предоставена под формата на:

1.устна справка;

2.писмена справка;

3.преглед на данните от самото лице;

4.предоставяне на исканата информация на технически и/или електронен носител.

(5) Администраторът на лични данни или изрично оправомощено от него длъжностно лице писмено уведомява заявителя за решението или отказа си по чл. 18, ал. 2 в съответния срок.

(6) Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни по образец съгласно ***Приложение № 4***, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

(7) Третите страни получават достъп до лични данни, обработвани в СУ „ Свети Паисий Хилендаски“ при наличие на законово основание за обработването на лични данни (напр. МОН, МВР, съд, прокуратура, НАП, НОИ и др.).

II. Мерки по осигуряване на защита на личните данни

Чл. 19.(1) ***Физическа защита*** в гимназията 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 гимназията 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.

1. 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.

(3) 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.

(4) 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.

(5) 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.

(6) Основните приложими технически мерки за физическа защита в гимназията включват използване на сигнално – охранителна система, ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства, които съответстват на изискванията на приложимата нормативна уредба.

Чл. 20. (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. задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни по образец (***Приложение № 5***);

Запознаване и осъзнаване на опасностите за личните данни, обработвани от СУ;

Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п.) между персонала и всякакви други лица, които са неоторизирани;

Деклариране на 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. 21. (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. 22. (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) Управление на ***външни връзки и/или свързване***, включващо от своя страна:

<u>Дефиниране на обхвата на вътрешните мрежи</u>: Като *вътрешни мрежи* се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на СУ. Като *външни мрежи* се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на ПГФР.

<u>Регламентиране на достъпа до вътрешната мрежа</u>: Достъп до вътрешната мрежа имат единствено служителите на СУ. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимо да знае“. Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола.

Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на лица с необходимата квалификация. В отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Администратора.

Контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация. Те са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на училището, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

Защитата от зловреден софтуер 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 оторизирани от директора на училището лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на ЗДАСД .

използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от директора на СУ лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.

активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.

4.Политиката по ***създаване и поддържане на резервни копия за възстановяване*** регламентира - Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на гимназията.

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 пропускателния режим 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 чийто срок за съхранение е изтекъл, се ***унищожават чрез приложим способ*** (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

9.Организация на телекомуникационните връзки и отдалечения достъп до вътрешните мрежи на СУ „Свети Паисий Хилендарски“:

1.Отдалечен достъп до вътрешни мрежи на СУ не е предвиден. По изключение, и след изричната оторизация от директора, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

2.Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от директора.

10.Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на САК, включват:

1.Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и забраната за разкриване на тайни пароли. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава

трафика в мрежа или опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно.

III. Базисни правила и мерки за осигуряване на защита на личните данни при компютърна обработка

Чл. 23. (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. 24. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране в разумна степен на устойчивост, 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 без устройствата, на които се съхраняват лични данни.

Чл. 25. (1) В гимназията се използва единствено софтуер с уредени авторски права.
(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице.
(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на лични данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 26. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица, респ. да споделят своя PIN с трети лица.

IV. Поддържани регистри и тяхното управление

Чл. 27. Поддържаните от СУ „ Свети Паисий Хилендарски“ регистри с лични данни са:

1. Ученици
2. Персонал
3. Родители
4. Доставчици
5. Дипломи
6. Пропускателен режим
7. Видеонаблюдение

Администратор на лични данни:
Средно училище „ Свети Паисий Хилендарски“
С. Скалица , ул. "Христо Ботев" № 2
uchilishte_skalitsa@abv.bg
Длъжността лице по защита на данните
Атанаска Минова Бонева
гр. Скалица, ул. " Христо Ботев" № 2
at_boneva@abv.bg, 0889018401

Чл. 28. (1) В регистър **„Ученици“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици“, обучавани в училището.

(2) Общо описание на регистър „Ученици“

Регистърът съдържа следните категории лични данни:

1.*Физическата идентичност* на лицето: име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка ;

2. ***Социална идентичност:*** информация за образование, документ за придобито образование, професионална квалификация,

3. Данни за здравословно състояние: медицинско свидетелство, имунизационен картон Нормативното основание е Законът за предучилищно и училищно образование и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на регистър „Ученици“:

1. носители на данни:

3.1.1. На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове в помещения на операторите на лични данни. Информацията от хартиените носители за всеки ученик, се записва в Книга за подлежащите на задължително обучение деца до 16-годишна възраст; Дневник за VIII - XII клас; Личен картон за дневна и индивидуална форма на обучение, Личен картон за задочна и самостоятелна форма на обучение ученически книжки, протоколи за провеждане на изпити, протоколи за резултати от изпити, със задължителни реквизити съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в същите помещения.

3.1.2. На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ Про. Базата данни се намира на твърдия диск на изолирани компютри.

3.1.3. Срок на съхранение: съгласно Номенклатурата на делата в училището със срокове на съхранение;

(4) Определяне на длъжностите:

1. Обработващи лични данни на регистър **„Ученици“** са: директор, ЗДУД, ЗДАСД, ЗАС, счетоводител и класни ръководители.
2. Оператор на лични данни на регистър **„Ученици“** е целия педагогически персонал.
3. Длъжностните лица – обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1.поверителност – високо ниво;
2.цялостност – високо ниво;
3.наличност – високо ниво;
4.общо за регистъра – високо ниво.

(6) ***Организационни мерки за физическа защита*** – определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. 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.

1.Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

(7) СУ „ Св. П. Хилендарски“ предприема превантивни действия при защита на личните Данни, като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от училището – предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
3. защита от наводнения- предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.
(8) Достъп до регистър „Ученици“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.
Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.
(***9) Лични данни на учениците*** се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в училището.
(10) След постигане целите по предходната алинея личните данни на учениците се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.
Чл. 29. (1) В регистър „**Родители**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързани с тях лица.
(2) Общо описание на регистър „Родители“
Регистърът съдържа следните групи данни:
1.физическата идентичност - име, ЕГН, адрес, телефони за връзка;
2. ***Социална идентичност:*** информация за образование;
3. ***Данни за здравословно състояние*** – Решения от ТЕЛК/НЕЛК и др. п.
Нормативното основание е Законът за предучилищно и училищно образование и приложимото законодателство, свързано с предоставянето на образователни услуги.
(3) Технологично описание на регистър „Родители“:
1. носители на данни:
3.1.1. На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в помещения на операторите на лични данни. Информацията от хартиените носители се записва в Книга за подлежащите на задължително обучение деца до 16-годишна възраст; Дневник за VIII - XII клас със задължителни реквизити съгласно НАРЕДБА № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование , които се съхраняват в същите помещения.
3.1.2. На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ Про. Базата данни се намира на твърдия диск на изолирани компютри.
3.1.3. Срок на съхранение: съгласно Номенклатурата на делата в ПГФР със срокове на съхранение;
(4) Определяне на длъжностите:
1. Обработващи лични данни на регистър **„Родители“** са: директор, ЗДУД, ЗДАСД, счетоводител, ЗАС и класни ръководители.
2. Оператор на лични данни на регистър **„Родители“** е целия педагогически персонал.
3. Длъжностните лица – обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.
(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:
1.поверителност – високо ниво;
2.цялостност – високо ниво;
3.наличност – високо ниво;

4.общо за регистъра – високо ниво.

(6) ***Организационни мерки за физическа защита*** – определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. 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.

1.Техническите мерки за физическа защита включват използване на ключалки, шкафове, както и оборудване на помещенията с пожарогасителни средства.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

(7) СУ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи – предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

3.защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(8) Достъп до регистър „Родители“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в ПГФР.

(10) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 30. (1) В регистър „**Персонал**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

(2) Общо описание на регистър „Персонал“

Регистърът съдържа следните групи данни:

1.физическата идентичност - име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка и банкови сметки;

2.психологическа идентичност – документи относно психическото здраве;

3.социална идентичност - образование и трудова дейност;

4.семейна идентичност - семейно положение и родствени връзки;

5.лични данни, които се отнасят до здравето;

6. лични данни относно съдебно минало – свидетелство за съдимост;

7. други - лични данни относно гражданско-правния статус на лицата.

Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

(3). Предназначението на събираните данни в регистъра е свързано с :

1.Индивидуализиране на трудовите правоотношения;

2.Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

3.Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.

4.Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(4) Технологично описание на регистър „Персонал“:

1.носители на данни:

4.1.1. На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудови досиета). Папките се подреждат в шкафове, които са разположени в помещения на операторите на лични данни.

4.1.2. На технически носител: Личните данни се въвеждат в специализирана счетоводна програма :счетоводство, ТРЗ и личен състав. Базата данни се намира на твърдия диск на изолирани компютри.

4.1.3. Срок на съхранение: съгласно Номенклатурата на делата в СУ „ Свети Паисий Хилендарски“ със срокове на съхранение;

(4) Определяне на длъжностите:

1. Обработващи лични данни на регистър **„Персонал“** са: директор, ЗДУД, ЗДАСД, счетоводител и ЗАС.

2. Оператор на лични данни на регистър **„Персонал“** е директорът.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1.поверителност – високо ниво;

2.цялостност – високо ниво;

3.наличност – високо ниво;

4.общо за регистъра – високо ниво.

(6) Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. 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.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

1. Трудовите досиета на персонала не се изнасят извън сградата на училището.

2. Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

3. При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на училището.

4. При внедряване на нов програмен продукт за обработване на лични данни се 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.

(7) СУ „ Свети Паисий Хилендарски“ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от училището – предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(8) Достъп до регистър „Персонал“ имат и държавните органи – НАП, НОИ, МОН, РУО за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.
(9) Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.
(10) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в СУ.
(11)След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 31. (1) В регистър „**Доставчици**“ В регистър „Доставчици“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица и/или юридически лица, съгласно Закона за счетоводството. Категориите физически лица и/или юридически лица, за които се обработват лични данни, са доставчици, с които работи училището.
(2)Общо описание на регистър „Доставчици“
Регистърът съдържа следните групи данни - физическата идентичност: трите имена, ЕГН, данни от личната карта, адрес, телефон и други, както и данни за юридически лица, включващи наименование, Булстат, материално отговорно лице, седалище и банкова сметка .
(3)Технологично описание на регистър „Доставчици“: Данните се набират в писмена форма в първични счетоводни документи.
(4)Определяне на длъжностите:
1. Обработващ лични данни на регистър **„Доставчици“** е счетоводител, ЗДАСД и ЗАС .
2. Оператор на лични данни на регистър **„Доставчици“** е директор .
(5)Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1.поверителност – ниско ниво;
2.цялостност – ниско ниво;
3.наличност – ниско ниво;
4.общо за регистъра – ниско ниво.

(6)Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(7) ПГФР предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1.защита при аварии, независещи от училището – предприемат се конкретни действия в зависимост от конкретната ситуация;

2.защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

3.защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(8) Достъп до регистър „Доставчици“: Категориите лица, на които личните данни могат да бъдат разкривани са физически лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт, на лица по силата на договор.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват.

(***10) След приключване на срока на съхранение*** , съгласно номенклатурата на делата, същите се унищожават физически, чрез изгаряне, след уведомяване на ДА.

(11)Източниците, от които се събират данните, са: от юридически и физически лица.

(12)Данните в регистъра се предоставят доброволно при съставяне на счетоводните документи.

Чл. 32. (1) Регистър **„Дипломи”** съдържа следните категории лични данни:

1.физическата идентичност на лицето: име, ЕГН, адрес, образ, паспортни данни, месторождение.

(2) В Регистър „Дипломи “ се въвеждат лични данни за следните документи:

- Диплома за средно образование (номенклатурен номер 3-34)
- Приложение към диплома за средно образование (обучение по модули) (номенклатурен номер 3-34.1)
- Дубликат на диплома за средно образование (номенклатурен номер 3-34А)
- Удостоверение за завършен гимназиален етап номенклатурен номер (номенклатурен номер 3-33)
- Дубликат на Удостоверение за завършен гимназиален етап (номенклатурен номер 3-33А)
- Приложение към удостоверение за завършен гимназиален етап (обучение по модули) (номенклатурен номер 3-33.1)
- Свидетелство за професионална квалификация (номенклатурен номер 3-54)
- Дубликат на Свидетелство за професионална квалификация (номенклатурен номер 3-54А)
- Приложение към свидетелство за професионална квалификация (обучение по модули) (номенклатурен номер 3-54.1)
- Диплома за средно образование (стар учебен план) – образец 3-36, 3-41 и 3-42
- Удостоверение за положен изпит по общообразователен предмет, не включен в дипломата за средно образование – образец 3-102
- Удостоверение за положен изпит по общообразователен предмет, не включен в дипломата за средно образование – образец 3-102 на ученици, които са завършили средното си образование в училища в чужбина.
- удостоверение за завършен клас - 3-103
- Удостоверение за преместване на ученик - 3-96

(3) Технологично описание на регистър „Дипломи за завършено средно образование“: носители на данни:

1.Информацията от хартиените носители за всеки ученик, се записва в Регистрационни книги за завършена степен на образование и/или професионална квалификация и се подреждат в шкафове в помещения на операторите на лични данни. Информацията за всеки ученик се записва в регистрационната книга със задължителни реквизити съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в същите помещения.

2. На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ Про. Базата данни се намира на

твърдия диск на изолирани компютри.
3. срок на съхранение: съгласно Номенклатурата на делата със срокове на съхранение;
(4) Определяне на длъжности:
1.Обработващи лични данни на регистър **„Дипломи“** са: директор, ЗДУД, ЗДАСД, ЗАС и класни ръководители.
2.Оператор на лични данни на регистър **„Дипломи“** е целия педагогически персонал.
3.Длъжностните лица – обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.
(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:
1.поверителност – високо ниво;
2.цялостност – високо ниво;
3.наличност – високо ниво;
4.общо за регистъра – високо ниво.
(6) Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. 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.
(7) Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.
Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.
(8) СУ „ Свети Паисий Хилендарски“ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:
1. защита при аварии, независещи – предприемат се конкретни действия в зависимост от конкретната ситуация;
защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
2. защита от наводнения- предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.
(9) Достъп регистър „Дипломи за завършено средно образование“ имат и държавните органи -МОН, РУО, за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове. Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.
Чл. 33. (1) В регистър **„Пропускателен режим“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица. Категориите физически лица, за които се обработват лични данни, са посетителите в сградата на училището.
(2) Общо описание на регистър „Пропускателен режим“:
1. Регистърът съдържа следните групи данни - физическата идентичност: име по лична карта
(3) Технологично описание на регистър „Пропускателен режим“:
Данните се набират в писмена форма в дневник.
(4) Определяне на длъжностите:
1.Обработващ лични данни на регистър „Пропускателен режим“ са чистачките и шофьра.

2.Оператор на лични данни на регистър „Пропускателен режим” е ЗДАСД.
(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:
1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;
4. общо за регистъра – ниско ниво.
(6) Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.
(7) Действия за защита при аварии, произшествия и бедствия: длъжностното лице изнася дневника при евакуация.
(8) Достъп до регистър „Пропускателен режим“: Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.
(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват (до приключване на дневника).
(10) След приключване на дневника, същият се унищожава физически, чрез изгаряне.
(11) Източниците, от които се събират данните, са: от физическите лица.
(12) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на училището.
Чл. 34. (1) В регистър „**Видеонаблюдение**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.
(2) Общо описание на регистър „Видеонаблюдение“:
Категориите физически лица, за които се обработват лични данни, са посетители, ученици, преподаватели и служители в сградите на гимназията.
Регистърът съдържа следните групи данни - физическата идентичност на лицето – видеообраз.
(3) Технологично описание на регистър „Видеонаблюдение“: Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на служителите и посетителите в сградата на гимназията.
(4)Определяне на длъжностите:
1.Оператори на лични данни на регистър **„Видеонаблюдение**“ са директор, ЗДУД, ЗДАСД.
(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:
1.поверителност – средно ниво;
2.цялостност – средно ниво;
3.наличност – средно ниво;
4.общо за регистъра – средно ниво.
(6) Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.
(***7) Категориите лица, на които личните данни могат да бъдат разкривани*** са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.
(***8) Лични данни се съхраняват*** в паметта на дивиара за срок до 30 дни. При необходимост записите могат да бъдат свалени на външен носител.
(9) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изтриване.
(10)Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на училището.
(11)На входовете на сградата се поставят информационни табла за уведомяване на гражданите, че при влизане и излизане от сградата подлежат на проверка съгласно чл. 30, ал.

1, т. 1, буква „а” и „б” от ЗЧОД и за използването на технически средства за наблюдение и контрол съгласно чл. 30, ал. 2 и ал. 4 от ЗЧОД.

V. Права и задължения на лицата, обработващи лични данни

Чл. 35. (1) (1) Длъжностно лице по защита на данните се определя от Ръководството на СУ „Свети Паисий Хилендарски“.

(2) Длъжностно лице по защита на данните има следните правомощия и длъжностни задължения:

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;

2.следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри с лични данни;

3. контрол по спазване на изискванията за защита на регистрите съобразно действащото законодателство и настоящите вътрешни правила;

4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;

5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;

6. специфицира техническите ресурси, прилагани за обработка на личните данни;

7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация на всички извършени действия с регистрите в компютърната среда;

8. определя ред за съхраняване и унищожаване на информационни носители;

9. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола;

10. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;

11. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

12. води регистър на дейностите по обработване на лични данни в СУ „Свети Паисий Хилендарски“ съгласно образеца в Приложение № 6.

Чл. 36. Служителите на СУ са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;

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 при необходимост регистрите на личните данни;

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.

Чл. 37. (1) За неспазването на разпоредбите на настоящите Вътрешни правила служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за училището или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство

VI. Допълнителни разпоредби

Чл. 38. Всички служители на училището са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заеманата от тях длъжност и възложената им работа.

Чл. 39. (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни,.

(2) Приложение към настоящите Вътрешни правила са образци на следните документи, съставяни при и по повод обработката на лични данни:

- **Приложение № 1** – *Декларация-съгласие за обработка на лични данни* (която се подписва, когато обработването не се извършва на друго основание, предвидено в чл. 6 от Регламент 2016/679);

- **Приложение № 2** – образец Протокол за задължителен инструктаж за запознаване с правилата за Противопожарна безопасност;

- **Приложение № 3 –** образец на Протокол за унищожаване на лични данни и носители на лични данни.

- **Приложение № 4** – Споразумение за обработка на данни;

- **Приложение № 5** - Протокол за преминато обучение по защита на личните данни и инструктаж за приложимите в САК правила и мерки за защита на личните данни;

- **Приложение № 6 –** Регистър на дейностите по обработка;

Преходни и заключителни разпоредби

§ 1. По смисъла на настоящите правила:

„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.

„**Администратор“** е физическо или юридическо лице, както и орган на държавната власт или на местното самоуправление, който сам или съвместно с друг определя целите и средствата за обработване на личните данни.

„**Администратор на лични данни**” е Средно училище „ Свети Паисий Хилендарски“ с. Скалица.

„**Ниво на защита**” е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.

„**Обработване на лични данни**“ е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

„**Обработващ лични данни**“ е лице, което обработва лични данни от името на администратора на лични данни.

„**Оператор на лични данни**” е всяко лице, което по указание и под ръководството на администратора има достъп до лични данни и упражнява ограничени функции по тяхната обработка съобразно нормативните актове, регламентиращи дейността на гимназията.

„Оценка на въздействие“ е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични

данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.
„**Поверителност**” е изискване за не разкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
„**Предоставяне на лични данни**“ са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.
„Регистър на лични данни“ е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.
„**Съгласие на физическото лице**“ е всяко свободно изразено, конкретно и информирано волеизявление, с което физическото лице, за което се отнасят личните данни, недвусмислено се съгласява, те да бъдат обработвани.
„**Трето лице**“ е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, различен от физическото лице, за което се отнасят данните, от администратора на лични данни, от обработващия лични данни и от лицата, които под прякото ръководство на администратора или обработващия имат право да обработват лични данни.

§2. Всички служители на училището са длъжни срещу подпис да се запознаят с Вътрешните правила и са длъжни да ги спазват.

§2. Вътрешните правила са утвърдени със Заповед № 0227/11.12.2018 година на директора