

ВЪТРЕШНИ ПРАВИЛА

на ОУ „Отец Паисий” град Разград

за мерките за защита на личните данни съгласно Регламент 2016/679

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Основно училище „Отец Паисий” е юридическо лице, което се състои от всички вписани в регистрите й адвокати и адвокати от Европейския съюз и е регистрирана по Закона за регистър БУЛСТАТ с БУЛСТАТ: 000498394.

(2) Основно училище „Отец Паисий” е със седалище в гр. Разград, ул. „Паисий” №6.

(4) Основно училище „Отец Паисий” обработва лични данни във връзка със своята дейност и сама определя целите и средствата за обработването им. В този случай училището действа като администратор на лични данни.

(5) В случаите, в които училището обработва лични данни за цели, определени самостоятелно от трето лице или целите са определени съвместно от училището и трето лице, училището има положението или на обработващ лични данни (ако целите са определени от лицето, което е възложило обработването) или на съадминистратор.

Чл. 2. Настоящите Вътрешни правила на Основно училище „Отец Паисий” уреждат организацията на обработване и защитата на лични данни на учителите и служителите, включително и на кандидатите за работа в училището, на контрагентите и партньорите, както и на всички други групи физически лица, с които училището влиза в отношения при осъществяването на правомощията и дейността си.

Чл. 3. (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) „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 комбинирание, ограничаване, изтриване или унищожаване.

(3) „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. 4. (1) Основно училище „Отец Паисий“ е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679.

(2) Като администратор на лични данни, при обработването на лични данни училището 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. 5. (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 Основно училище „Отец Паисий“, не изискват или вече не изискват идентифициране на субекта на данните, училището 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. 6. Основно училище „Отец Паисий“ 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 на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. Основно училище „Отец Паисий” прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи и мрежи;
5. Криптографска защита.

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. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на Основно училище „Отец Паисий” и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на Основно училище „Отец Паисий” се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл. 9. Когато не са налице хипотезите на чл. 6, пар. 1, б. „б“ – „е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от Основно училище „Отец Паисий”, подписват декларация за съгласие по образец.

Чл. 10. (1) Право на достъп до регистрите с лични данни имат само органите на Основно училище „Отец Паисий”, съобразно възложените им от закона правомощия и оторизираните учители и служители на училището, 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 защитата на данните.

(2) Оторизирането на учители и служители се извършва на база длъжностна характеристика или чрез изричен акт на Директора на Основно училище „Отец Паисий”.

(3) Учителите и служители 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 учители и служители.

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

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

(2) Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив, за срокове, съобразени с действащото законодателство. Помещенията, определени за архив, са оборудвани с пожарогасители и задължително се заключват.

(3) Документите на електронен носител се съхраняват на специализирани сървъри, 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 с цел осигуряване на възможност 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.

(4) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизираните лица и органите на Основно училище „Отец Паисий” съобразно възложените им от закона правомощия.

Чл. 12. (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.

Чл. 13. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от Основно училище „Отец Паисий” регистри. Проверките се извършват от комисия, включваща учители и служители на училището, които изготвят Доклад за резултата от проверката.

(2) Докладът по ал. 1 трябва да включват преценка на необходимостта за обработка на личните данни или унищожаване. Докладите се адресират до Директора на училището.

Чл. 14. (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 прекия си ръководител, 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. 15. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, Основно

училище „Отец Паисий” може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на 2 години или при промяна на характера на обработваните лични данни.

Чл. 16. (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от Основно училище „Отец Паисий” 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, Основно училище „Отец Паисий” 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 служители, упълномощени с изричен писмен акт на директора на училището 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

Чл. 17. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, Основно училище „Отец Паисий” съобщава в 1-месечен срок от подаване на заявлението, респ. искането.

(3) 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.

(4) 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

(5) Третите страни получават достъп до лични данни, обработвани в Основно училище „Отец Паисий”, при наличие на законово основание за обработването на лични.

II. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 18. Физическата защита в Основно училище „Отец Паисий” се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 19. (1). Основните *организационни мерки за физическа защита* в Основно училище „Отец Паисий” включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни,
3. определяне на организацията на физическия достъп;

(2) Като *помещения, в които ще се обработват лични данни*, се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за учители и служители и с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява „непублична“ част, в която се извършват дейностите по обработване на лични данни, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и „публична част“ – до която имат достъп външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

(3) *Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове*, 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 извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.*

(5) *Зони с контролиран достъп* са всички помещения на територията на Основно училище „Отец Паисий”, в които се събират, обработват и съхраняват лични данни.

(6) *Използваните технически средства за физическа защита на личните данни в Основно училище „Отец Паисий” са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на работните им задължения.*

(7) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал.

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

Чл. 20. (1). Основните *технически мерки за физическа защита* в Основно училище „Отец Паисий” включват:

1. използване на сигнално-охранителна техника;
2. Използване на ключалки и заключващи механизми;
3. шкафове, метални каси,
4. оборудване на помещенията с пожарогасителни средства.

(2) Документите, съдържащи лични данни, се съхраняват в *шкафове или картотеки, които могат да се заключват*, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафите притежават единствено изрично натоварените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика).

(3) *Оборудването на помещенията*, където се събират, обработват и съхраняват лични данни, включва: сигнално-охранителна техника, *ключалки* за ограничаване на достъпа единствено до оторизираните лица; заключваеми шкафове и пожарогасителни средства.

(4) *Пожарогасителните средства* се разполагат в съответствие с изискванията на приложната нормативна уредба.

Чл. 21. (1). Основните *мерки за персонална защита* на личните данни, приложими в Основно училище „Отец Паисий”, 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 преминат инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни;
2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от Основно училище „Отец Паисий”;
3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п..) между персонала и всякакви други лица, които са неоторизирани;

Чл. 22. (1). Основните *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 Основно училище „Отец Паисий” , сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;

2. *Определяне на условията за обработване на лични данни* - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната бизнес дейност на Основно училище „Отец Паисий”, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;
3. *Регламентиране на достъпа до регистрите с лични данни* – достъпът до регистрите с лични данни 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 не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.
5. *Процедури за унищожаване*: Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на Основно училище „Отец Паисий” или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

(2) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 1, се прилагат и следните допълнителни мерки:

1. *Контрол на достъпа до регистрите*, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае”, за да изпълняват техните задължения;
2. *Правила за размножаване и разпространение*, които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

Чл. 23. (1) *Защитата на автоматизираните информационни системи и/или мрежи* в Основно училище „Отец Паисий” 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, включват:

1. *Идентификация и автентификация* чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на Основно училище „Отец Паисий”. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе 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 водене, поддръжка и обработка;

3. Управление на външни връзки и/или свързване, включващо от своя страна:

- Дефиниране на обхвата на вътрешните мрежи: Като *вътрешни мрежи* се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на училището. 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 училището.
- Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служителите и/или специално упълномощени лица. 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 минимизиране 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.

4. *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 Ръководството на училището лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на ИТ специалиста на училището.
- използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от Ръководството на училището 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.

- забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми оторизираните от Ръководството на училището лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.
5. Политика по създаване и поддържане на резервни копия за възстановяване, която регламентира:
- Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на училището.
 - Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.
 - Отговорност за архивиране има лицето, обработващо личните данни.
 - Срокът на архивиране следва да е съобразен с действащото законодателство.
 - Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа
6. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.
7. 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).
- (3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 2 се прилагат и допълнителни мерки, свързани с:
1. *Организация на телекомуникационните връзки и отдалечения достъп* до вътрешните мрежи на Основно училище „Отец Паисий” :
 - Отдалечен достъп до вътрешни мрежи на Основно училище „Отец Паисий” не е предвиден. По изключение, и след изричната оторизация от Ръководството на училището, 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.
 - Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от Ръководството на САК.
 2. Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на САК, включват:
 - Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на училището от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието,

адекватността на използваните мерки и способности за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

- Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на училището, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. 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, а ако нарушението е не само дисциплинарно или представлява престъпление – и по предвидения за санкциониране на това нарушение/престъпление ред.

3. Мерките, свързани със създаване на *физическа среда (обкръжение)*, включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способности), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Чл. 24. (1) По отношение на личните данни се прилагат и мерки, свързани с *криптографска защита на данните* чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на комуникационното оборудване.

(2) Криптирането се използва и за защита на личните данни, които се предават от училището по електронен път или на преносими носители.

III. БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 25. (1) Компютърен достъп през локалната мрежа 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 име и парола към системата. При приключване на работното време служителите изключват локалния си компютър. В

(2) САК прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност повече от 30 секунди), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.

(5) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от училището период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(6) Системите, обработващи и/или съхраняващи лични данни, включват система за контрол, регистрираща следните действия в журнал (log) за одит: опити за влизане и ефективно влизане и излизане от системата, действията на потребителите в процеса на всяка работна сесия, смяна на пароли. Когато бъде установена нетипична активност (например влизане в нетипично време, неизключане на работна станция след изтичане на работното време и др.п.), системният администратор незабавно уведомява Ръководството и Длъжностното лице по защита на данните за извършване на проверка по случая.

Чл. 26. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

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

Чл. 27. (1) В Основно училище „Отец Паисий” се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано от Ръководството на училището лице. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(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 личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 28. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

IV. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 29. Поддържаните от Основно училище „Отец Паисий” регистри с лични данни са:

I. „Персонал”

- Директорът, като юридическо лице, което се явява администратор на лични данни по смисъла на ЗЗЛД и обработват личните данни на работника/служителя за изпълнение на своите нормативни задължения във връзка с трудовите и осигурителните отношения, включително данъчни задължения, социално и здравно осигуряване, безопасни и здравословни условия на труд, счетоводно отчитане и др., както и в изпълнение на други общи нормативни задължения на работодателя.

Използването на данните за други цели, които не влизат в нормативните задължения на работодателя, трябва да стане със съгласието на работника/служителя.

Работодателят – администратор на лични данни, е длъжен да не разкрива личните данни на работника/служителя на трети лица. Предоставяне и достъп до тези данни може да има само в случаите, когато работодателят е нормативно задължен да предостави данните на съответните публични органи и организации или му е надлежно изискана от такива органи по съответния ред.

Данните се обработват и съхраняват на хартиен и електронен носител. Работодателят – администратор на лични данни, се задължава да осигури необходимите технически и организационни мерки за защита на данните от посегателства, загуба или промени.

Физическите лица:

Обработващият личните данни е задължен да осъществява защита на личните данни при обработването и осъществяването на достъпа до тези данни, като осигури защитата на личните данни, сигурността и конфиденциалността на информацията.

При ръчното обработване на личните данни, лицата се задължават да предприемат надлежни мерки, за да се предотврати непозволен достъп или разкриване, промяна, унищожаване или случайна загуба.

Администраторът и обработващите данните, не носят отговорност ако работникът/служителят сам е оповестил публично личните си данни на трети лица.

II. „Контрагенти“

III. „Ученици“

Лицата се задължават да обработват личните данни,

- Законосъобразно и добросъвестно
- Да събират личните данни за конкретни, точно определени и законни цели и да не обработват личните данни допълнително, по начин несъвместим с тези цели
- Да отразяват личните данни точно и при необходимост да се актуализират
- Да заличават или коригират ЛД, когато се установи, че са неточни или непропорционални по отношение на целите за които се обработват
- Да поддържат ЛД във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите.

Горепосочените лица за водене на регистър се задължават да гарантират надеждност на обработването, като осигурят технически и организационни мерки за защита на личните данни срещу:

- случайно или незаконно разрушаване
- незаконно разкриване или достъп
- случайна загуба или промяна
- нерегламентирано изменение или разпространение, както и всички други незаконни форми на обработване
- незаконно копиране, изнасяне и разпространяване
- изтриване (унищожаване) преди изтичане на необходимия срок за съхранение, съответстващ само на целите, за които те са събрани и се обработват.

V. „Видеонаблюдение“

VI. „Свидетелства за завършено основно образование“ се води от ЗАС – Милена Колева.

Обработващият личните данни е задължен да осъществява защита на личните данни при обработването и осъществяването на достъпа до тези данни, като осигури защитата на личните данни, сигурността и конфиденциалност на информацията.

При ръчното обработване на личните данни, лицата се задължават да предприемат надлежни мерки, за да се предотврати непозволен достъп или разкриване, промяна, унищожаване или случайна загуба.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 30. (1) Длъжностно лице по защита на данните се определя от Ръководството на училището.

(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. осъществява 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 и/или криптографски ключ;
10. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, за 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 училището

Чл. 31. Служителите на ОУ „Отец Паисий” 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. 32. (1) За неспазването на разпоредбите на настоящите Вътрешни правила учителите и 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. 33. Всички учители и служители на ОУ „Отец Паисий” са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

Чл. 34. 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,.

Чл. 35. Настоящите вътрешни правила са приети с решение на ПС № от 2018 г.

Директор:
(Мирослав Минков)