52 ОУ „Цанко Церковски“

София, кв. Бояна, бул. „Ал. Пушкин“ 112, тел./факс (02) 855-20-54

УТВЪРЖДАВАМ,
ДИРЕКТОР:

/М. Димитрова/

ИНСТРУКЦИЯ

за мерките за защита на личните данни

I. Общи положения

Чл. 1. (1) 52 ОУ „Цанко Церковски“ е юридическо лице със седалище гр. София, 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. Настоящата инструкция урежда организацията на обработване и защитата на лични данни на преподавателите, служителите, обучаемите (ученици), посетителите, както и на други физически лица, свързани с осъществяването на нормалната дейност на училището.

Чл. 3. (1) Като „обработване на лични данни“ се възприема 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 на данните.

(2) Обработването на лични данни се състои и в осигуряване на достъп на 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. 3, ал.1 от Закона за защита на личните данни и е вписано в регистъра на администраторите на лични данни и на водените от тях регистри на личните данни по чл. 10, ал.1, т.2 от ЗЗЛД.

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

(2) Принципите за защита на личните данни са:

1.Принцип на ограничено събиране – събирането на лични данни трябва да бъде в рамките на необходимото. Инфорамцията се събира по законен и обективен начин;

2. Принцип на ограниченото използване, разкриване и съхраняване – личните данни не трябва да се изплзват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели;

3. Принцип на прецизност – личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за изпълнението на тези цели;

4. Принцип на сигурността и опазването – личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

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

Чл. 7. (1) 52 ОУ „Цанко Церковски" 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. 8. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

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

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

Чл. 9. Физическите лица, чиито лични данни се обработват, подписват декларация за съгласие по образец. (Приложение №2).

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

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

(3) Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено

нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции.

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

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

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

(3) Съхранението на документите и преписките на хартиен носител, архвирането/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/оператоара на лични данни с оглед запазване на информацията за съответните лица в актуален вид и възможността й за възстановяване, в случай на погиване на основния носител/система. Архивните копия сес 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. 12. С оглед за щита на хартиените, техническите и и нформационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Чл. 13. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, служителят констатирал това нарушение, докладва писмено за този инцидент на училищното ръководство.

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

Чл. 14. (1) При повишаване нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й училището може да определи друго ниво на защита за регистъра.

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

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

(3) Унищожаване се осъществява от служителя, оотговорен за архива на училището.

Чл. 16. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на зявление (Прилижение №3), респективно искане за достъп на информация, и след тяхното летитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, училището съобщава в 30 дневен срок от подаване на заявлението.

(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) Изключение се допуска единствено на тези органи и/или институции, които извършват това въз основа на искане на закона (например: МОН, МВР, съд, прокуратура, НАП, НОИ и други).

II. Мерки по осигуряване на защита на личните данни

Чл. 17.(1) Физическа защита в училището се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни

(2) Основните приложими организационни мерки за физическа защита в училището включват определяне на помещенията, в които ще се обработват и съхраняват лични данни, включително и определяне на организацията на физически достъп.

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

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

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

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

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

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

Чл. 18. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

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

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

(4) Лицата могат да започнат да обработват лични дани след запознаване със:
1. нормативната уредба в областта на защита на личните данни;
2. политиката и ръководствата за защита на личните данни;
3. опасностите за личните данни, обработвани от администратора.

Чл. 19. (1). Основните приложими мерки за документална защита на личните данни са:
1. Определяне на регистрите, които ще се подържат 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 нормална 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 целта за която са били събирани и /или изискванията на действащото законодателство.
5. Процедури за унищожаване: документите съдържащи лични данни, които не подлежат на издаване към Държавен архив и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на училището, се унищожават по подходящ и сигурен начин (нарязване, електронно изтриване и други подходящи за целта методи).

Чл. 20. (1) Защитата на автоматизираните информационни системи и/или мрежи в училището включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информациони 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 училищет. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразени 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, подръжка и обработка;
3.Защитата от вируси, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системния, а при възможност и приложния софтуер се контролира, инсталира и подържа от ръководител компютърен кабинет.
4. Политиката по създаване и подържане на резервни копия за възстановяване регламентира -- Основната цел на архивирането е свързана с прдотвратяването на загуба на информация, свързана с лични данни, която би зтруднила нормалното функциониране на училището.

5. Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители.
6. Персоналната защита на данните е част от цялостната охрана на училището.
7. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.
8. Данните, които вече не са необходими за целите на училището и чиито срок за съхранение е изтекъл, се унищожават чрез приложим способ.

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

Чл.21. (1) Компютърен достъп към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определен 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. Вслучай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват.

Чл. 22. (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 небходимост от ремонт на компютърна техника, предоставянето и на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 23. (1) В училището се използва единствено софтуер с уредени авторски права.
(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано 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 Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

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

IV. Подържани регистри и тяхното управление

Чл. 25. Подържаните от 52 ОУ „Цанко Церковски регистри с лични данни са:
1. Ученици
2. Персонал
3. Родители
4. Пропускателен режим
5 Видеонаблюдение

Чл. 26. (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“
Регистъра съдържа следните категории лични данни:
1. физическа идентичност на лицето: име, ЕГН, адрес, месторождение, телефони за връзки;
2. културна идентичност: интереси;

3. социална идентичност – образование;
4. семейна идентичност – родствени връзки;
5. лични данни, които се отнасят до здравето.
Нормативното основание е Законът за предучилищно и училищно образование и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на регистър „Ученици".

- Носители на данни:

- На хартиен носител: Данните се набират в писмена (документална форма) и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се 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 ПГ;Дневник за 1-4 клас; Дневник за 5-7 клас; Дневник за ЦДО
- На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация „Админ". Базата данни се намира на твърдия диск на изолирани компютри.
- Срок на съхранение: съгласно номенклатурата на 52 ОУ със срокове на съхранение;

(4) Определяне на длъжностите:
Обработващи лични данни на регистър „Ученици" са: Директор, зам. директор УД, , ЗАС, класни ръководители и технически сътрудник.
Оператор на лични данни на регистър „Ученици: е целия педагогически персонал.
Длъжностните лица – обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните дани.

(5) Нивото на въздействие на регистъра по отношение на различните критериие, 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 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. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на лужебните 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 контрол на достъпа.
Техническите 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 подържане на антивирусни програми, периодично архивиране на външен носител, както и чрез подържане на информацията и на хартиен носител.

(7) 52 ОУ „Цанко Церковски" предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили събития, а именно:
1. защита при аварии, независещи от 52 ОУ – предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари – незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответние органи;
3. защита от наводнения – предприемат се ограничаване на разпространението;

(8) Достъп до регистър „Ученици" имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане", ДАЗД 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 52 ОУ „Цанко Церковски".

(10) След постигане на предходната алинея личните данни на учениците се унищожават физически, за което се изготвят актови протоколи за унищожаване.

Чл.27. (1) В регистър „Родители" се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързанис тях лица.

(2) Общо описание на регистър „Родители"

Регистърът съдържа следните групи данни:

1. физическа идентичност – име, ЕГН, адрес, телефони за връзка и месторабота;
2. социална идентичност – образование, трудова дейност;
3. семейна идентичност – семейно положение и родствени връзки.

Нормативно основание е Законът за предучилищно и училищно образование и приложимото законодателство, свързано с предоставянето на обаразователни услуги.

(3) Технологично описание на регистър „Родители".

➢ носители на данни:

- На хартиен носител: Даните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на операторите на лични данни,снабдени със защитна сигнализация. Информацията от хартиените носители се записва в Книга за подлежащите на задължително обучение; Дневници за ПГ,1-4 клас, 5-7 клас, ЦДО, ресурсно подпомагане със задължителни реквизити.
- На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ. Базата данни се намира на твърдия диск на изолирани компютри.
- Срок на съхранение: съгласно Номенклатурата със срокове на съхранение.

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Родители" са: главен счетоводител,ЗАС и класни ръководители.

Оператор на лични данни на регистър „Родители" е целия педагогически персонал.

Длъжностните лица – обработващи лични данни и оператори на лични данни предприемат всички организационно – технически мерки са съхраняването и опазването на личните данни.

(5) Нивото на въздействие на регистъра по отношение на различните критериие, 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 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. Достъп се предоставя само на служители, 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.
Защитата на електронните данни от неправомерен достъп се осъществява посредством подържане на антивирусни програми, периодично архивиране на външен носител, както ичрез подържане на информацията и на хартиен носител.

(7) 52 ОУ „Цанко Церковски" предприема превантивни действия при защита на личните дани като съставя план за действие при различните случаи на настъпили събити, а именно:
1. защита при аварии, независещи от 52 ОУ – предприемат се онкретни действия в зависимост от конкретната ситуация;
2. защита от пожари – незабавно гасене със собствени средства и уведомяване на съответните органи;
3. защита от наводнения – предприемат действия по ограничаване на разпространението, както и изпомпване и изгребване;

(8) Достъп до регистър „Родители" имат и държавните органи – МОН, РУО, ДАЗД, дирекция „Социално подпомагане" за изпълнение на техните задължения, предвдени в съответните законови и подзаконови 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 52 ОУ.

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

Чл. 28. (1) В регистър „Персонал" се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или по граждански договори.

(2) Общо описание на регистър „Персонал"
Регистърът съдържа следните групи данни:
1. физическата идентичност – име, ЕГН, адрес, данни по л.к., месторождение, телефони за връзки 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. 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.
Предназначението на събираните данни в регистъра е свързано с:
1. Индивидуализиране на трудовите правоотношения;
2. Изпълнение на нормативнитв 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 други.
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.

(3) Технологично описание на регистър „Персонал":

➢ носители на данни:

- 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 изолирани заключващи се помещения на операторите на лични данни снабдени със защитна сигнализация.
- На технически носител: Личните данни се въвеждат в специализирана счетоводна програма: счетоводство. Базата данни се намира натвърдия диск на изолорани компютри.
- Срок на съхранение: съгласно Номенклатурата със срокове на съхранение.

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Персонал" са зам. директор АСД, главен счетоводител и СЧР.

Оператор на лични данни на регистър „Персонал" е зам. директор УД.

(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 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. 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 заключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

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

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

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.

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

(7) 52 ОУ „Цанко Церковски" предприема превантивни действия при защита на личните данни като съставя план за действие при при различните случаи на настъпили извънредни събития, а именнно:

1. защита при аварии, независещи от 52 ОУ – предприемат се конкретни действия в зависимост от ситуацията;
2. защита от пожари -- незабвно гасене със собствени средства и уведомяване на съответните органи;
3. защита от наводнения – предприемат се действия по ограничаване на разпространението;

(8) Достъп до регистър „Персонал" имат и държавните органи -- НАП, НОИ, МОН, РУО за изпълнение на техните здължения, предвидени в съответните законови и подзаконови актове. Достъп до обработваните лични данни имат и съответните държавни органи – съд, следсвие, 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 52 ОУ.

(10) След постигане целите на прдходната алинея личните данни се унищожават физически, за което се изготвят актови протоколи за унищожаване.

Чл. 29. (1) В регистър „Пропускателен режим" се набира и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Категориите физически лица, за които се обработват лични данни, са посетителите в сградата на училището.

(2) Общо описание на регистър „Пропускателен режим"

Регистърът съдържа следните групи данни – физическа идентичност: имена по лична карта и адрес.

(3) Технологично описание на регистър " Пропускателен режим": Данните се набират в писмена форма в дневник.

(4) Определяне на длъжностите:

Обработващ лични данни на регистър „Пропускателен режим" е охранителя/портиера.

(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, проишествия 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 физическита 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 и спазване на законовия срок за съхранение, същият се унищожава физически.

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

(12) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на училището.

(13) На входовете на сградата се поставят информационни табели за уведомяване на гражданите за пропускателния режим в сградата и проверка съгласно чл. 56, ал.1,2 и 3 от ЗЧОД, както и за използването на технически средства за наблюдение и контрол, съгласно същия чл. 56.

Чл. 30. (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 обработават лични данни, са посетители, ученици, преподаватели и служители в сградите на училището.

Регистърът съдържа следните групи данни – физическа 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 училището.

(4) Определяне на длъжностите:

Оператори на лични данни на регистър „Видеонаблюдение са: Директор, зам. директор УД, педагогическия персонал и охранителя.

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

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 огараничен 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 от 1 месец.
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. 56, ал. 1, т.1, ал. 2, ал. 3 от ЗЧОД и за използване на технически средства за наблюдение и контрол съгласно чл. 56, ал.1, т. 1 букви „в“ и „г“ от ЗЧОД.

V. Права и задължения на лицата, обработващи лични данни

Чл. 31. (1) Лице по защита на лични данни е Директорът на училището.

(2) Лицето по защита на лични данни има следните правомощия:

1. осигурява организация по водене на регстрите, 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 реигстри;
3. осъществява контрол по спазване на изискванията за защита на регистрите;
4. подържа 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. опреля ред за съхраняване и унищожаване на информационни носители;
9. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхото отстраняване.

(3) Лицето по защита на личните данни може да делегира своите пълномощия изцяло и/или чстично на други лица.

Чл. 32. Служителите на училището 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 цел ;
3. да актуализират регистрите на личните данни (при необходимост);

4. да заличават или корегират личните данни, когато се установи, че са неточни или непропорционални за целите, за които се обработват;
5. да подържат личните данни във вид, който позволява идентифициране насъответните физически лица за период не по дълъг от необходимия за целите за които тези данни се обработват; задълженията си.

Чл. 33. (1) За неспазването на разпоредбите на настоящата инструкция, служителите носят административна отговорност.

(2) Ако в резултат на действията на съответния служител по обработване на лични данни, са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по - тежко деяние, за което се предвижда наказателна отговорност.

Преходни и заключителни разпоредби

1. По смисъла на настоящата инструкция:

- **„Лични данни“** са всяка информация, отнасяща се до физическо лице, което е идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.
- **„Администратор“** е физическо лице, както и орган на държавната власт или на местното самоуправление, който сам съвместно с друг определя целите и средствата за обработване на личните данни.
- **„Администратор на лични данни“** е 52 ОУ „Цанко Церковски“,София.
- **„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 училището.
- **„Оценка на въздействие“** е процес за определяне на 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, цялостната или наличността на личните данни.
- **„Поверителност“** е изискване за неразкриване 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 на 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“ /субекта/** е всяко свободно изразено, конкретно и информирано заявена воля, 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 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 инструкцията и да я спазват.

3. Инструкцията се издава на основание на Регламент ЕС 2016/679 на европейския парламент и на Съвета от 27.04.2016г. за защита на личните данни.

4. За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Закона за защита на личните данни,