Средно училище
"Свети свети Кирил и Методий"

Асеновград

ул."Княгиня Евдокия" №41 тел/факс: 0331/6 47 87
e-mail:info-1600116@edu.mon.bg http://www.susskm.com

ЗАПОВЕД
N РД-10-2853/10.09.2026 г.

На основание чл.258, ал.1 от ЗПУО и чл.237 от Закона за защитата на личните данни

1.УТВЪРЖДАВАМ

Вътрешни правила за защитата на личните данни
в СУ „Св.св.Кирил и Методий", гр.Асеновград

Длъжностно лице за защитата на личните данни - **Георги Иванов Анастасов.**

2.ОПРЕДЕЛЯМ:

Лица, отговарящи за регистърите – *Приложение 10*

Заповедта да се доведе до занието на лицата за сведение и изпълнение.

МАЯ КРАЕВА

Директор на СУ „ Св.св.Кирил
и Методий", гр.Асеновград

Средно училище
"Свети свети Кирил и Методий"

Асеновград

ул."Княгиня Евдокия" №41
e-mail:info-1600116@edu.mon.bg
тел/факс: 0331/6 47 87
http://www.susskm.com

Утвърдил:

МАЯ КРАЕВА

Директор на СУ „Св.св.Кирил и Методий", гр.Асеновград

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

СУ „СВ. СВ. КИРИЛ И МЕТОДИЙ"

ГР. АСЕНОВГРАД

Раздел I. Общи положения

Чл. 1. (1) СУ „Св. св. Кирил и Методий“ е юридическо лице със седалище и адрес на управление: гр.Асеновград, ул.“Княгиня Евдокия“ 41 Република България, с основна дейност образование и образователни услуги, наричано по-долу **„Училището“**.

(2) Училището е **администратор на лични данни** по смисъла на чл. 4, т. 7 от Регламент (ЕС) 2016/679, доколкото самостоятелно или съвместно с други лица определя целите и средствата за обработване на лични данни.

(3) Училището обработва лични данни във връзка с изпълнение на своите образователни, възпитателни, административни, трудовоправни, счетоводни, архивни, здравно-превантивни и охранителни функции.

Чл. 2. (1) Настоящите вътрешни правила уреждат организацията, реда, отговорностите и мерките за защита при обработване на лични данни на:

1. ученици;
2. родители, настойници, попечители и други законни представители;
3. педагогически специалисти;
4. служители и работници;
5. кандидати за работа;
6. посетители;
7. контрагенти, представители и лица за контакт;
8. дарители;
9. участници в проекти, програми, състезания, олимпиади, стажове и практики;
10. други физически лица, чиито лични данни се обработват във връзка с дейността на Училището.

(2) Целта на правилата е да осигурят законосъобразно, добросъвестно, прозрачно и сигурно обработване на лични данни и да въведат вътрешна организация за спазване на Регламент (ЕС) 2016/679, Закона за защита на личните данни и приложимото специално законодателство.

(3) Правилата уреждат:

1. принципите и основанията за обработване;
2. реда за водене на регистър на дейностите по обработване;
3. техническите и организационните мерки за защита;
4. реда за достъп до лични данни;
5. реда за упражняване на права от субектите на данни;
6. реда за действие при нарушения на сигурността;
7. задълженията на служителите;
8. ролята на длъжностното лице по защита на данните;

9. правилата за видеонаблюдение;
10. правилата при използване на електронни системи, НЕИСПУО, електронна поща, облачни услуги и други информационни ресурси;
11. правилата при възлагане на обработване на външни лица.

Чл. 3. Настоящите правила се прилагат за всяка операция или съвкупност от операции с лични данни, извършвани чрез автоматични или неавтоматични средства, включително събиране, записване, организиране, структуриране, съхранение, промяна, извличане, справка, употреба, разкриване чрез предаване, ограничаване, изтриване или унищожаване.

Чл. 4. По смисъла на настоящите правила:

1. **„лични данни“** са всяка информация, свързана с идентифицирано или подлежащо на идентифициране физическо лице;
2. **„субект на данни“** е физическото лице, за което се отнасят личните данни;
3. **„обработване“** е всяка операция или съвкупност от операции с лични данни;
4. **„администратор“** е Училището, когато определя целите и средствата за обработването;
5. **„обработващ лични данни“** е физическо или юридическо лице, публичен орган или друга структура, която обработва лични данни от името на Училището;
6. **„получател“** е физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват лични данни;
7. **„нарушение на сигурността на личните данни“** е нарушение, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни;
8. **„специални категории лични данни“** са данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, генетични данни, биометрични данни за целите на уникална идентификация, данни за здравословното състояние, сексуалния живот или сексуалната ориентация.

Раздел II. Принципи и правни основания за обработване

Чл. 5. (1) Личните данни се обработват при спазване на следните принципи:

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) Училището обработва лични данни само когато е налице поне едно от следните правни основания:

1. обработването е необходимо за спазване на законово задължение, приложимо спрямо Училището;

2. обработването е необходимо за изпълнение на задача от обществен интерес или при упражняване на официални правомощия, предоставени на Училището;

3. обработването е необходимо за изпълнение на договор или за предприемане на действия преди сключване на договор;

4. обработването е необходимо за защита на жизненоважни интереси на субекта на данните или на друго физическо лице;

5. субектът на данните е дал съгласие за конкретна цел;

6. когато е приложимо и Училището не действа като публичен орган при изпълнение на своите задачи — обработването е необходимо за легитимен интерес на администратора или трета страна, при условие че не преобладават правата и свободите на субекта на данните.

(3) Съгласие се използва само когато няма друго приложимо правно основание и когато субектът на данните разполага с реална свобода да даде, откаже или оттегли съгласието си без неблагоприятни последици.

(4) При обработване на лични данни на деца Училището прилага повишено внимание, ясна информация и засилени мерки за защита.

Чл. 6. (1) Специални категории лични данни се обработват само когато е налице основание по чл. 6 от Регламент (ЕС) 2016/679 и приложимо изключение по чл. 9, пар. 2 от Регламент (ЕС) 2016/679.

(2) Здравни данни на ученици и служители се обработват само доколкото това е необходимо за изпълнение на законови задължения, защита на жизненоважни интереси, обществен интерес в областта на общественото здраве, трудовото и социалното законодателство, предоставяне на здравна грижа или друга правно допустима цел.

(3) Данни за съдебно минало или удостоверяване на липса на обстоятелства, несъвместими със заемане на длъжност, се обработват само когато това е изрично предвидено в закон.

Раздел III. Организация на обработването

Чл. 7. (1) Училището обработва лични данни само за конкретни, изрично указани и легитимни цели.

(2) Не се допуска обработване на лични данни за цели, несъвместими с първоначалните цели, освен ако е налице законово основание или валидно съгласие.

(3) Служителите обработват лични данни само в обем, необходим за изпълнение на служебните им задължения.

Чл. 8. (1) Училището поддържа **Регистър на дейностите по обработване**, съгласно Приложение № 3.

(2) Регистърът съдържа най-малко:

1. данни за администратора;
2. данни за длъжностното лице по защита на данните;
3. целите на обработването;
4. категориите субекти на данни;
5. категориите лични данни;
6. категориите получатели;
7. информация за предаване към трети държави или международни организации, когато е приложимо;
8. срокове за съхранение;
9. общо описание на техническите и организационните мерки;
10. оценка на риска;
11. необходимост от оценка на въздействието.

(3) Регистърът се преглежда най-малко веднъж годишно и при всяка съществена промяна в дейностите по обработване.

Чл. 9. (1) Поддържаните регистри в училището са:

1. Трудови правоотношения
2. Болнични листове и временна неработоспособност
3. Подбор на персонал
4. Проекти „Еразъм+“ и други международни проекти
5. Видеонаблюдение
6. Основна образователна дейност

7. Документация, свързана с образователната дейност

8. Издаване на удостоверения, свидетелства и дубликати

9. Квалификация на персонала

10. Прием на ученици

11. Трудова медицина

12. Здравно обслужване на ученици

13. Служебни бележки, справки и удостоверения за служители

14. Дарения

15. Изпити

16. Състезания, олимпиади и конкурси

17. Стипендии

18. Производствени практики, стажове и обучение в реална работна среда

19. Национални програми и проекти

20. Библиотека

21. Обща и допълнителна подкрепа за личностно развитие

22. Счетоводство

23. Архив

24. Входящ регистър

25. Изходящ регистър

26. Регистър на договорите

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

(3) Всяка година Директорът издава заповед, с която определя лицето/служителят, който да отговаря за всеки отделен регистър (дейност).

(4) За всеки регистър се оценява рискът по следния начин:

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

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

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

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

(5) При „изключително високо ниво на риск“, констатирано при условията на предходната алинея, се извършва „Оценка на въздействието“ спрямо начина и критериите, залегнали в Регламент (ЕС) 2016/679 и настоящите правила.

Чл. 10. (1) Директорът със заповед или в длъжностна характеристика определя служителите, които имат право на достъп до конкретни категории лични данни и до конкретни дейности по обработване.

(2) Достъп се предоставя само при наличие на служебна необходимост и при спазване на принципа **„необходимост да се знае“**.

(3) При прекратяване на трудово или служебно отношение, промяна на длъжност или отпадане на необходимостта от достъп, правата за достъп се прекратяват незабавно.

Чл. 11. (1) Училището обработва информация и документи в системата на предучилищното и училищното образование чрез НЕИСПУО и други интегрирани информационни продукти, когато това е предвидено в нормативен акт.

(2) Достъпът до НЕИСПУО се предоставя само на лица, определени със заповед на директора, съобразно служебните им функции.

(3) Подаването и въвеждането на данни в НЕИСПУО се извършва по установения нормативен ред и, когато се изисква, с квалифициран електронен подпис.

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

Чл. 12. (1) Училището определя длъжностно лице по защита на данните, наричано по-долу **ДЛЗД**.

(2) Координатите за връзка с ДЛЗД се публикуват по подходящ начин и се съобщават на КЗЛД.

(3) ДЛЗД участва във всички въпроси, свързани със защитата на личните данни.

(4) Длъжностното лице по защита на данните е длъжно:

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

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

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

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

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

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

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

з) да си сътрудничи с надзорния орган;

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

й) ДЛЗД може да дава и други съвети, ако притежава необходимата компетентност, стига да не водят до конфликт на интереси.

(5) ДЛЗД има право:

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

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

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

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

(6) При изпълнение на своите задачи ДЛЗД действа напълно независимо и свободно от указанията на Администратора на лични данни

(7) ДЛЗД не може да бъде санкционирано или освобождавано заради изпълнение на функциите си.

(8) ДЛЗД не взема оперативни решения относно целите и средствата за обработване и не замества администратора.

Чл. 13. (1) Служителите на училището са длъжни:

1. да обработват лични данни законосъобразно, добросъвестно и прозрачно;

2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;

3. да актуализират регистрите на личните данни (при необходимост);

4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

6. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си;

7. незабавно да уведомяват администратора на лични данни в случай, че установят нарушение на сигурността на лични данни, независимо дали при извършване на своята работа или при друго лице, което обработва лични данни.

(2) За неспазването на разпоредбите на Настоящите вътрешни правила служителите носят административна, дисциплинарна отговорност по Кодекса на труда, административно-наказателна, а в определени случаи и наказателна отговорност.

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

Раздел V. Обработващи лични данни и трети лица

Чл. 14. (1) Когато Училището възлага обработване на лични данни на външен изпълнител, се сключва писмен договор или се включва клауза за обработване на лични данни.

(2) Договорът с обработващия урежда най-малко:

1. предмета и срока на обработването;
2. естеството и целта на обработването;
3. вида лични данни;
4. категориите субекти на данни;
5. правата и задълженията на Училището;
6. задължение обработващият да действа само по указания на Училището;
7. задължение за поверителност;
8. технически и организационни мерки;
9. подпомагане на Училището при упражняване на права от субектите;
10. подпомагане при нарушения на сигурността;
11. ред за използване на подизпълнители;
12. изтриване или връщане на данните след приключване на услугата;
13. право на проверки и одит.

(3) Обработващият не може да включва друг обработващ без предварително писмено разрешение на Училището.

Чл. 15. Когато Училището и друго лице съвместно определят целите и средствата на обработването, отношенията се уреждат с договореност между съвместни администратори,

която определя правата и задълженията им, включително точка за контакт за субектите на данни.

Раздел VI. Права на субектите на данни

Чл. 16. Субектите на данни имат следните права, доколкото са приложими:

1. право на информация;
2. право на достъп;
3. право на коригиране;
4. право на изтриване;
5. право на ограничаване на обработването;
6. право на възражение;
7. право на преносимост, когато е приложимо;
8. право да не бъдат обект на изцяло автоматизирано решение, включително профилиране, когато е приложимо;
9. право на жалба до КЗЛД;
10. право на съдебна защита.

Чл. 17. (1) Исканията за упражняване на права се подават писмено, електронно или устно.

(2) Когато искането е устно, служителят, който го приема, съставя протокол, който се подписва от заявителя и служителя.

(3) Субектът на данните не е длъжен да използва образците към настоящите правила.

(4) Училището може да поиска допълнителна информация за потвърждаване на самоличността на заявителя, когато има основателни съмнения.

(5) Работниците/служителите в училището трябва да оказват съдействие на всички субекти на данните.

(6) Във всеки един случай Администраторът на лични данни следва да потърси становището на ДЛЗД или друго компетентно лице.

Чл. 18. (1) Училището отговаря на искането без ненужно забавяне и най-късно в срок **1 месец** от получаването му.

(2) При необходимост срокът може да бъде удължен с още **2 месеца**, като заявителят се уведомява в едномесечен срок от получаване на искането, заедно с причините за удължаването.

(3) Когато Училището не предприема действия по искането, уведомява заявителя за причините и за правото му на жалба до КЗЛД и съдебна защита.

(4) Информацията и действията по исканията се предоставят безплатно, освен когато исканията са явно неоснователни или прекомерни.

Чл. 19. Правото на изтриване не се прилага, когато обработването е необходимо за:

1. спазване на правно задължение;
2. изпълнение на задача от обществен интерес или официални правомощия;
3. архивиране в обществен интерес;
4. установяване, упражняване или защита на правни претенции;
5. обществен интерес в областта на общественото здраве;
6. други случаи, предвидени в приложимото законодателство.

Раздел VII. Информиране на субектите на данни

Чл. 20. (1) Училището предоставя информация на субектите на данни чрез:

1. публикуване на интернет страницата на Училището;
2. поставяне на информационни съобщения на достъпни места;
3. предоставяне на хартиени или електронни известия при поискване;
4. включване на информация в заявления, договори, формуляри и други документи при необходимост.

(2) Информацията се предоставя в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език.

(3) Информация, насочена към ученици, се предоставя по начин, съобразен с тяхната възраст и разбиране.

Чл. 21. (1.1) Известие за обработване на лични данни на ученици и родители се съдържа в Приложение № 5. Информацията, съдържаща се в известието по Приложение № 5, се публикува на интернет страницата на училището, както и на хартиен носител до входа, като се пригоди в необходимия формат и наименува коректно.
(1.2) Копие от известието се дава на ученик, а когато е непълнолетен - съответно негов родител, само при изрично искане за това и срещу подпис от тяхна страна на екземпляр, който остава в училището.

(2.1) Известие за обработване на лични данни на служители и кандидати за работа се съдържа в Приложение № 6. Информацията, съдържаща се в известието по Приложение 6, се публикувана интернет страницата на училището, само ако има секция достъпна единствено за служители/работници в училището, както и на хартиен носител в учителската стая и счетоводството.
(2.2) Копие от известието се дава на работник/служител срещу подпис от негова страна на екземпляр, който остава в училището.
(3) Подписването на известие удостоверява запознаване, а не представлява съгласие, освен когато в отделна част изрично се иска съгласие за конкретна незадължителна цел.

Раздел VIII. Съгласие

Чл. 22. (1) Когато обработването се основава на съгласие, то се събира чрез отделна декларация или ясно потвърждаващо действие.

(2) Искането за съгласие се представя отделно от други въпроси, в разбираема и лесно достъпна форма, с ясен и прост език.

(3) Съгласието може да бъде оттеглено по всяко време.

(4) Оттеглянето не засяга законосъобразността на обработването преди оттеглянето.

(5) Оттеглянето трябва да бъде толкова лесно, колкото даването на съгласие.

(6) Мълчание, предварително отметнати полета или липса на действие не представляват съгласие.

(7) Училището съхранява доказателства за дадено съгласие за срока на обработване и доколкото е необходимо за доказване на законосъобразността му.

Раздел IX. Сигурност на личните данни

Чл. 23. Училището въвежда подходящи технически и организационни мерки, като отчита естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица.

Чл. 24. Мерките за защита включват:

1. физическа защита;
2. персонална защита;
3. документална защита;
4. защита на автоматизирани информационни системи и мрежи;
5. контрол на достъпа;
6. управление на потребителски права;
7. архивиране и възстановяване;
8. антивирусна защита;
9. защита на преносими носители;
10. криптиране, когато е приложимо;
11. журнални записи, когато системата позволява;
12. обучение на персонала;
13. процедури при инциденти;
14. периодичен преглед и актуализация.

Раздел X. Физическа защита

Чл. 25. (1) Физическата защита се осигурява чрез ограничаване на достъпа до помещенията, в които се обработват или съхраняват лични данни.

(2) Помещенията за съхранение на документи се заключват.

(3) Достъп до помещенията имат само служители, на които това е необходимо за изпълнение на служебните задължения.

(4) Когато в помещенията имат достъп външни лица, се обособява непублична зона.

(5) Архивните помещения следва да са сухи, проветриви, защитени от пряка слънчева светлина, оборудвани с пожарогасителни средства и с ограничен достъп. Те следва да са физически ограничени и достъпни само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения. Създава се подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система, както и сигнално-охранителна техника.

Раздел XI. Персонална защита

Чл. 26. (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:

- познаване на нормативната уредба в областта на защитата на личните данни;
- познаване на политиката и ръководствата за защита на личните данни;
- знания за опасностите за личните данни, обработвани от администратора;
- поемане на задължение за неразпространение на личните данни, изразено в декларация по образец. (Приложение 4).

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае". „Необходимост да знае" означава, че закон, друг нормативен акт или естеството на работата изисква лицето да получава дадена информация или без нея изпълнението на служебните му задължения би се затруднило неимоверно много или стане невъзможно.

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

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

(5) Работници/служители имат право на достъп до регистрите с лични данни на база длъжностна характеристика или чрез изричен акт/заповед Директора.

(6) Работниците/служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни.

(7) Нарушенията на правилата могат да водят до дисциплинарна, административнонаказателна, гражданска или наказателна отговорност.

Раздел XII. Документална защита

Чл. 27. (1) Документи, съдържащи лични данни, се създават, получават, съхраняват, архивират и унищожават съобразно нормативните срокове и вътрешната номенклатура на делата, като 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.

(2) Документи с лични данни не се оставят без надзор на публично достъпни места.

(3) Достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае".

(4) Изнасяне на документи извън Училището се допуска само:

1. когато е предвидено в закон;
2. за нуждите на компетентен орган;
3. по изрично писмено разрешение на директора;

(5) За всяко изнасяне и връщане на документи извън училището се изготвя предавателно-приемателен протокол, в който се описват документите, определя се срокът за използване и се декларира ангажиментът за връщането им в архива.
(6) При установяване на липси и увреждания след връщането на документите се съставя протокол и писмено се уведомява директора.
(7) Лицето, отговарящо за съответните документи или за архива, ако са архивни, проверява състава и състоянието на документите преди и след използване.

(8) Процедури за унищожаване: Документите, съдържащи лични данни, които не подлежат на предаване 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, който не позволява възстановяване на данните (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи). За всяко такова унищожаване се съставя протокол.

(9) Определяне на срокове за съхранение - документите с 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

Раздел XIII. Защита на информационните системи

Чл. 28. (1) Достъп до електронни системи, файлове и бази данни с лични данни се предоставя само чрез индивидуален потребителски профил.

(2) Не се допуска използване на чужди потребителски имена, пароли, електронни подписи или средства за удостоверяване.

(3) Паролите се съхраняват поверително и се променят периодично.

(4) При три неуспешни опита за достъп, когато системата позволява, профилът се заключва.

(5) При прекратяване на основанието за достъп профилът се деактивира незабавно.

Чл. 29. (1) На служебните компютри се използва само разрешен софтуер.

(2) Не се допуска инсталиране на неразрешен софтуер или използване на средства за заобикаляне на защитата.

(3) Информационните системи се защитават с антивирусен софтуер, защитна стена и други подходящи средства.

(4) При съмнение за зловреден софтуер служителят незабавно прекратява работа със системата и уведомява директора, системния администратор и ДЛЗД.

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

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

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

3. Защитата от вируси, включва:

- използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от ръководител направление ИКТ.

- 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 Директора и оторизираните от него 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.

4. Политиката по създаване и поддържане на резервни копия за възстановяване има за цел предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на училището.

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

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

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

8. Следва да има определено лице, което да извършва периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните

9. Данните, които вече не са необходими за целите на училището и чиито срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. постоянно заличаване от електронните средства или друг приложим метод отговарящ на съвременните софтуерни изисквания, чието използване следва да бъде документирано).

(6) 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.

(7) 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. при необходимост и чрез изтриване на акаунта).

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

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

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

(11) В училището се използва единствено софтуер с уредени авторски права.

(12) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице – ръководител направление ИКТ.

(13) 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.

(14) 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, неизключване на работна станция след изтичане на работното време и др.п.), системният администратор незабавно уведомява Директора и Длъжностното лице по защита на данните за извършване на проверка по случая.

(15)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 работниците/служителите и/или специално упълномощени от Директора 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.

• На работници/служители на училището може да бъде предоставен Интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до електронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка на Директора, съгласувана с оторизираните Директора лица, отговарящи за мрежите и защитата им, за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове.

Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на Директора, както и в случаите на заплаха за сигурността на данните.

• Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от Директора или посочено от него лице.

(16) Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на училището, 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 способи 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 работници/служители 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 оперираш 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.

• По отношение на личните данни по възможност 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. Криптирането се използва и за защита на личните данни, които се предават от училището по електронен път или на преносими носители.

Чл. 30. (1) Създават се резервни копия на електронни данни, когато това е необходимо за осигуряване на непрекъсваемостта на дейността.

(2) Резервните копия се съхраняват защитено и достъпът до тях е ограничен.

(3) Преносими носители, съдържащи лични данни, се използват само при служебна необходимост и при подходящи мерки за защита.

Чл. 31. (1) Отдалечен достъп до системи с лични данни се допуска само по разпореждане на директора и при технически мерки за защита.

(2) Публикуване на информация в интернет, съдържаща лични данни, се извършва само след проверка на правното основание, обема на данните и необходимостта от публикуване.

Раздел XIV. Видеонаблюдение

Чл. 32. (1) Училището може да извършва видеонаблюдение с цел:

1. защита на живота и здравето на ученици, служители и посетители;
2. опазване на имуществото;
3. предотвратяване и установяване на инциденти;
4. защита на документи, архиви и информационни ресурси;
5. съдействие на компетентни органи в предвидените от закона случаи;
6. когато нормативен акт изисква това.

(2) Видеонаблюдението се извършва само в необходимия обхват и при спазване на принципа за свеждане на данните до минимум.

(3) Не се допуска видеонаблюдение в санитарни помещения, съблекални, стаи за почивка, медицински кабинет, помещения за индивидуална психологическа или педагогическа подкрепа, освен ако закон изрично не предвижда друго.

(4) Не се извършва звукозапис, освен ако има изрично правно основание, оценка на въздействието и предварително информиране.

(5) На входовете и в наблюдаваните зони се поставят информационни табели.

(6) Записите се съхраняват до **30 дни**, освен ако конкретен запис е необходим за разследване на инцидент, защита на права или изпълнение на законово задължение.

(7) Достъп до записите имат само лица, определени със заповед на директора.

(8) Предоставяне на записи на МВР, прокуратура, съд, РУО, община или други органи се извършва само при законово основание и се документира.

(9) За видеонаблюдението се поддържа отделна част в Регистъра на дейностите по обработване.

(10) При промяна в обхвата, броя камери, зоните или срока за съхранение се извършва преглед на риска и при необходимост оценка на въздействието.

Раздел XV. Системи за контрол, вътрешни ресурси и докладване

Чл. 33. (1) Училището може да използва системи за контрол на достъпа, работното време, трудовата дисциплина, ползването на служебна електронна поща, интернет, служебна техника и други вътрешни ресурси само при ясни правила, съразмерност и предварително уведомяване на служителите.

(2) Служебните електронни пощи, компютри, платформи и технически средства се използват само за служебни цели, освен ако директорът е разрешил ограничено лично ползване.

(3) Проверка на служебни електронни ресурси се допуска само при служебна необходимост, спазване на пропорционалност и документиране на проверката.

(4) При въвеждане на вътрешна система за подаване на сигнали се приемат отделни правила, включващи обхват, достъп, срокове, поверителност и права на засегнатите лица.

Раздел XVI. Нарушения на сигурността на личните данни

Чл. 34. (1) Всеки служител, който установи или има съмнение за нарушение на сигурността на личните данни, уведомява незабавно прекия си ръководител, директора и ДЛЗД.

(2) Нарушение може да бъде:

1. изгубен документ;
2. изгубен или откраднат носител;
3. изпратен имейл до неправилен адресат;
4. неправомерен достъп до система;
5. зловреден софтуер;
6. публикуване на лични данни без основание;
7. предоставяне на данни на неупълномощено лице;
8. загуба, промяна, унищожаване или неразрешено разкриване на данни;
9. всяка друга дейност, която може да се приеме като разпространяваща или загубваща лични данни без да има основание за това.

Чл. 35. (1) За всяко нарушение се съставя запис в регистър на нарушенията.

(2) Регистърът съдържа:

1. дата и час на установяване;
2. лице, установило нарушението;
3. описание на нарушението;
4. категории засегнати данни;
5. категории и приблизителен брой засегнати лица;
6. вероятни последици;

7. предприети мерки;
8. оценка на риска;
9. решение дали се уведомява КЗЛД;
10. решение дали се уведомяват субектите;
11. мотиви, когато не се уведомява КЗЛД или субектите.

Чл. 36. (1) ДЛЗД подпомага директора при оценката дали нарушението има вероятност да доведе до риск за правата и свободите на физическите лица.

(2) Когато има вероятност за риск, директорът уведомява КЗЛД без ненужно забавяне и по възможност до 72 часа от узнаването.

(3) Когато уведомяването е извършено след 72 часа, се посочват причините за забавянето.

(4) Уведомлението до КЗЛД съдържа:

1. описание на нарушението;
2. категории и приблизителен брой засегнати лица;
3. категории и приблизителен брой засегнати записи;
4. данни за контакт с ДЛЗД;
5. вероятни последици;
6. предприети или предложени мерки.

(5) Когато нарушението може да доведе до висок риск за правата и свободите на физическите лица, директорът уведомява и засегнатите лица без ненужно забавяне.

Раздел XVII. Оценка на риска и оценка на въздействието

Чл. 37. (1) За всяка дейност по обработване се извършва оценка на риска, като се отчитат:

1. естеството на данните;
2. дали се обработват данни на деца;
3. дали се обработват здравни данни или други специални категории;
4. броят на засегнатите лица;
5. обемът на данните;
6. срокът за съхранение;
7. достъпът на трети лица;
8. използването на нови технологии;
9. вероятните последици при нарушение;
10. вероятността от неправомерен достъп, загуба или разкриване.

(2) Нивата на риск са:

1. **нисък риск**;
2. **среден риск**;
3. **висок риск**;
4. **много висок риск**.

Чл.38. (1) Оценка на въздействието върху защитата на данните се извършва, когато вид обработване има вероятност да доведе до висок риск за правата и свободите на физическите лица.

(2) Оценка на въздействието се извършва задължително и когато обработването попада в списък на операции, за които КЗЛД е определила такава оценка като необходима.

(3) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.

(4) Оценка на въздействието се извършва преди започване на обработването.

(5) ДЛЗД дава становище по оценката.

Раздел XVIII. Съхранение, архивиране и унищожаване

Чл. 39. (1) Личните данни се съхраняват само за сроковете, необходими за постигане на целите на обработването, или за сроковете, предвидени в закон, подзаконов нормативен акт, номенклатура на делата или архивни правила.

(2) След изтичане на срока за съхранение данните се изтриват, унищожават или архивират, когато това е предвидено в закон.

(3) Унищожаването на хартиени документи се извършва чрез шредиране или друг метод, който не позволява възстановяване.

(4) Унищожаването на електронни данни се извършва чрез трайно изтриване, презаписване, криптографско заличаване или физическо унищожаване на носителя.

(5) За унищожаването се съставя протокол.

Чл. 40. При преобразуване, закриване или промяна в структурата на Училището предаването на документи и лични данни на друг администратор се извършва само при наличие на правно основание, приемо-предавателен протокол и при спазване на приложимите архивни правила.

Раздел XIX. Обучение и контрол

Чл. 41. (1) Всички служители се запознават с настоящите правила срещу подпис.

(2) При необходимост се провеждат обучения относно:

1. основни принципи на защита на личните данни;
2. сигурност на информацията;

3. работа с документи;
4. действия при инциденти;
5. работа с НЕИСПУО и други електронни системи;
6. видеонаблюдение;
7. права на субектите.

Чл. 42. (1) Директорът осъществява общ контрол по прилагането на правилата.

(2) ДЛЗД наблюдава съответствието и дава препоръки.

(3) Системният администратор или определено техническо лице осъществява контрол върху техническите мерки, без да получава достъп до съдържанието на лични данни извън необходимото за поддръжка.

Чл. 43. Когато се работи онлайн или се преминава към ОРЕС следва да се спазват, освен настоящите правила, и издадените за това правила, с които се запознават всички участници в процеса.

Раздел XX. Преходни и заключителни разпоредби

§ 1. Настоящите правила са задължителни за всички педагогически специалисти, служители, работници и лица, които обработват лични данни по възлагане от Училището.

§ 2. Правилата се утвърждават със заповед на директора и влизат в сила от датата на утвърждаването им.

§ 3. За всички неуредени въпроси се прилагат Регламент (ЕС) 2016/679, Законът за защита на личните данни, Законът за предучилищното и училищното образование, Законът за здравето, Законът за Националния архивен фонд, Кодексът на труда, Кодексът за социално осигуряване, Законът за счетоводството и приложимите подзаконови нормативни актове.

§ 4. Настоящите правила отменят предходни вътрешни инструкции и правила за защита на личните данни, доколкото им противоречат.

§ 5. За видеонаблюдение и други специфични дейности могат да се издават допълнителни правила относно тях.

§ 6. Изменения и допълнения се извършват със заповед на директора, след становище на ДЛЗД.

§ 7. Всички изменения се свеждат до знанието на служителите срещу подпис.

Приложение № 1.

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ

Долуподписаният/ата……
……ЕГН: ……

Адрес/контакт: ……

ДЕКЛАРИРАМ, ЧЕ:

Давам свободно, конкретно, информирано и недвусмислено съгласие …… да обработва следните мои лични данни:

……
……
……

за следната конкретна цел:

……
……
……

Информиран/а съм, че:

1. предоставянето на съгласие е доброволно;
2. мога да откажа да дам съгласие без неблагоприятни последици, освен ако без данните не може да бъде изпълнена конкретната доброволна дейност;
3. мога да оттегля съгласието си по всяко време;
4. оттеглянето не засяга законосъобразността на обработването преди оттеглянето;
5. данните ще се съхраняват за срок: ……;
6. получатели/категории получатели са: ……;
7. имам право на достъп, коригиране, изтриване, ограничаване, възражение и жалба до КЗЛД.

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

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

Дата: …… ДЕКЛАРАТОР:……

гр./с……..

Приложение № 2.

ЗАЯВЛЕНИЕ ЗА УПРАЖНЯВАНЕ НА ПРАВА ПО РЕГЛАМЕНТ (ЕС) 2016/679

До Директора на .....

От:.....
ЕГН/ЛНЧ:.....
Адрес за кореспонденция:.....
Телефон/e-mail: .....

В качеството ми на:
☐субект на данни
☐ родител/настойник/попечител на .....
☐ пълномощник, с приложено пълномощно

Моля да упражня следното право:

☐ достъп до лични данни
☐ копие от лични данни
☐ коригиране
☐ изтриване
☐ ограничаване на обработването
☐ възражение
☐ преносимост, когато е приложимо
☐ друго: .....
Описание на искането:

.....
.....
.....
.....

Предпочитана форма за отговор:

☐ на хартиен носител
☐ по електронна поща
☐ друго: .....

Дата: ..... г.

Подпис: .....

Получено от:.....

на ..... г.

Приложение № 3.

РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Администратор: .....
Адрес:.....
Тел.:.....
E-mail: .....

Длъжностно лице по защита на данните: .....
E-mail:.....
Тел.: .....

1. Описание на регистъра.

2. Лица с достъп.

3. Източник / Описание на дейността по събиране на лични данни.

4. Цели на събирането.

5. Законово основание.

6. Категории лични данни, които се обработват.

7. Категории субекти на лични данни.

8. Получатели на лични данни.

9. Трансфер.

10. Срок.

11. Локация на личните данни.

12. Общо описание на техническите и организационните мерки за сигурност.

13. Оценка на риска.

14. Изисква ли се оценка на въздействие? Ако да – оценката.

1. Трудови правоотношения

1. **Описание:** обработване на данни при възникване, изпълнение, изменение и прекратяване на трудови правоотношения.
2. **Лица с достъп:** директор, счетоводител, ЗАС, заместник-директори.
3. **Източник:** служителят, публични органи, документи по трудовото правоотношение.
4. **Цели:** администриране на трудовото правоотношение, възнаграждения, осигуряване, отпуски, дисциплинарна отчетност, квалификация.
5. **Основание:** чл. 6, пар. 1, т. "Б" от ОРЗД – сключване на трудовия договор и произхождащото от него трудово правоотношение, както и законовите задължения чл. 6, пар. 1, б. „в" ОРЗД; КТ, КСО, данъчно и осигурително законодателство; за специални категории — чл. 9, пар. 2, б. „б" ОРЗД.
6. **Категории данни:** име, ЕГН, номер и дата на издаване на лична карта,N на лична карта, адрес, семейно положение и деца (в определени случаи: лични данни на съпруг/съпруга и други близки за упражняване на трудови права, напр. при отпуски по майчинство), информация за трудовия стаж и професионалния опит (включително заемани длъжности, работно време, стаж по специалността), информация за банкови сметки, заплата и социални придобивки, месторабота, информация за подбор (включително копия от разрешителни за работа, препоръки и друга информация, посочени в автобиография и придружително писмо или предоставена по друг начин в процеса на кандидатстване, информация относно трудова дисциплина, данни за образование и квалификация.

   Специални категории: членство в синдикални организации, тъй като това е предвидено задължение в закона. Данни за съдебно минало, присъди и нарушения се обработват отделно и само когато това е изрично предвидено в закон/свидетелство за съдимост/.
7. **Субекти:** настоящи и бивши работници/служители.
8. **Получатели:** НАП, НОИ, банки, МОН/РУО/община, Инспекция по труда, други компетентни органи.
9. **Трансфер:** няма, освен ако конкретен проект/дейност не изисква друго правно основание.
10. **Срок:** съгласно номенклатурата на делата; ведомости за заплати — 50 години; трудови досиета и свързани документи — съгласно приложимите срокове.
11. **Локация:** канцелария/архив, определени със заповед; електронни системи с ограничен достъп.
12. **Мерки:** охрана на сградата, видеонаблюдение, контролиран достъп до тях - Директор, ЗАС, администратор, домакин - пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни.
13. **Риск:** среден.
14. **ОВЗД:** не, освен при въвеждане на нова система за систематичен контрол или мащабно наблюдение.

2. Болнични листове и временна неработоспособност

1. **Описание:** приемане и обработване на болнични листове и документи за временна неработоспособност.
2. **Лица с достъп:** директор, специалист ТРЗ, счетоводител, ЗАС.
3. **Източник:** служителят, електронни системи/компетентни органи, когато е приложимо.
4. **Цели:** удостоверяване на неработоспособност, администриране на отпуск, обезщетения и осигурителни задължения.
5. **Основание:** чл. 6, пар. 1, б. „в“ ОРЗД; КТ, КСО и приложимите към тях нормативни актове; чл. 9, пар. 2, б. „б“ ОРЗД.
6. **Категории данни:** имена, ЕГН, длъжност, здравословно състояние, период на неработоспособност, здравна информация в болничния лист.
7. **Субекти:** работници/служители.
8. **Получатели:** НОИ, НАП, ТЕЛК/НЕЛК, компетентни органи.
9. **Трансфер:** няма.
10. **Срок:** съгласно КСО, счетоводни и архивни правила; отделно от трудовите досиета.
11. **Локация:** кабинет на ТРЗ/архив.
12. **Мерки:** охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, шкаф с ключ, копие от който имат хората, които работят с тях — специалист ТРЗ, Счетоводител, директор, длъжностно лице отговарящо за архивохранилището, определено със Заповед на Директор и Директорът, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни. Болничните листове се съхраняват отделно от трудовите досиета на работниците/служителите.
13. **Риск:** среден.
14. **ОВЗД:** не.

3. Подбор на персонал

1. **Описание:** подбор на кандидати за работа и поддържане на необходимата в тази връзка документация.
2. **Лица с достъп:** директор, заместник-директори, счетоводител, домакин, комисия по подбор, ЗАС при необходимост други работници/служители, които участват в даден подбор.
3. **Източник:** кандидатът.
4. **Цели:** оценка на кандидатура, провеждане на подбор, сключване на трудов договор.
5. **Основание:** чл. 6, пар. 1, б. „б“ ОРЗД; договорно основание.
6. **Категории данни:** имена, ЕГН, адрес, контакти, образование, квалификация, професионален опит, информация за трудовия стаж и професионалния опит

(включително заемани длъжности, работно време, стаж по специалността), информация за подбор (включително копия от разрешителни за работа, препоръки и друга информация, посочени в автобиография и придружително писмо или предоставена по друг начин чрез процеса на кандидатстване), информация относно трудова дисциплина, документи за правоспособност, автобиография, документи, изискуеми по закон.

7. **Субекти:** кандидати за работа.
8. **Получатели:** комисия по подбор, МОН/РУО/община или контролен орган при проверка.
9. **Трансфер:** няма.
10. **Срок:** до 12 месеца от приключване на подбора, освен при съгласие за по-дълъг срок или специален закон.
11. **Локация:** канцелария.
12. **Мерки:** охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, шкаф с ключ, копие от който имат хората, които работят с тях — ЗАС, Счетоводител, директор, длъжностно лице отговарящо за архивохранилището, определено със Заповед на Директор и Директорът, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни, унищожаване след срока.
13. **Риск:** нисък до среден.
14. **ОВЗД:** не.

4. Проекти „Еразъм+“ и други международни проекти

1. **Описание:** участие на ученици и служители в международни проекти по ЕРАЗЪМ+.
2. **Лица с достъп:** Директор, Счетоводител, домакин, ЗАС, ръководителят на проекта, МОН, учители определени със заповед на директора, участващи в проекта и организатори или участници, имащи законен достъп до лични данни и упълномощените потребители на електронната деловодна система.
3. **Източник:** от самите субекти – например от участници, родители, проектни документи.
4. **Цели:** кандидатстване, изпълнение, отчетност, мобилност, пътуване, застраховане, настаняване, комуникация с партньори, осъществяване на самия проект и поддържане на необходимата документация, свързана с него.
5. **Основание:** чл. 6, пар. 1, б. „б“, „в“ и „д“ ОРЗД; проектни договори и правила на програмата; съгласие за незадължителни публикации.
6. **Категории данни:** имена, ЕГН/дата на раждане, клас/длъжност, контакти, документ за самоличност при пътуване, образование, квалификация, банкови данни при разходи, здравни данни само ако са необходими за безопасност/пътуване.
7. **Субекти:** ученици, родители, служители.

8. **Получатели:** ЦРЧР, Европейска комисия/платформи, партньорски организации, транспортни, застрахователни и настаняващи организации, банки.
9. **Трансфер:** в ЕС/ЕИП — по правилата на ОРЗД; към трети държави — само при подходящи гаранции или приложимо изключение.
10. **Срок:** съгласно проектния договор и правилата за отчетност; обичайно 5 години след приключване, ако не е предвиден друг срок.
11. **Локация:** кабинет на заместник-директори/счетоводство/проектна папка/електронна система.
12. **Мерки:** ограничен достъп, договорни клаузи, минимизиране, криптиране при електронно изпращане.
13. **Риск:** среден.
14. **ОВЗД:** преценка според проекта; при специални категории/трети държави — допълнителна оценка.

5. Видеонаблюдение

1. **Описание:** видеонаблюдение в общи части, входове, коридори, двор и други определени зони.
2. **Лица с достъп:** директор и лица, определени със заповед.
3. **Източник:** видеокамери.
4. **Цели:** сигурност, опазване на живот, здраве и имущество, предотвратяване и установяване на инциденти. Опазване имуществото на училището, в това число и всички документи, повечето от които съдържат лични данни.
5. **Основание:** чл. 6, пар. 1, б. „д“ и/или „в“ ОРЗД; при приложимост — легитимен интерес само за дейности извън публични задачи.
6. **Категории данни:** изображение, дата, час, място. Не се обработва звук.
7. **Субекти:** ученици, служители, посетители.
8. **Получатели:** МВР, прокуратура, съд, МОН, други компетентни органи при законово основание.
9. **Трансфер:** няма.
10. **Срок:** до 30 дни, освен при инцидент и зписи от ДЗИ/2 месеца/ и НВО.
11. **Локация:** защитен записващ носител/сървър в заключено помещение.
12. **Мерки:** табели, ограничен достъп, пароли, протокол при преглед/копиране/предоставяне.
13. **Риск:** среден; висок при разширен обхват или систематично мащабно наблюдение.
14. **ОВЗД:** при мащабно систематично наблюдение, нова система, аудио или разширен обхват.

6. Основна образователна дейност

1. **Описание:** обучение, оценяване, дневници, комуникация с ученици и родители.

2. **Лица с достъп:** директор, заместник-директори, учители, класни ръководители, педагогически специалисти.
3. **Източник:** ученици, родители, учители, НЕИСПУО.
4. **Цели:** организация на обучението, оценяване, присъствия, отсъствия, комуникация, изпълнение на ЗПУО.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД; ЗПУО, Наредба № 8/11.08.2016 г. на МОН и приложимите нормативни актове.
6. **Категории данни:** имена, ЕГН/дата на раждане, адрес, клас, оценки, отсъствия, контакт с родители, образователни данни.
7. **Субекти:** ученици, родители.
8. **Получатели:** МОН, РУО, община, НЕИСПУО, други органи по закон.
9. **Трансфер:** няма.
10. **Срок:** съгласно Наредба № 8 и номенклатурата; дневници — 5 години, документи с дългосрочна стойност — до 50 години или постоянно.
11. **Локация:** НЕИСПУО, училищни електронни системи, архив.
12. **Мерки:** индивидуален достъп, служебни профили, ограничаване по класове/роля на потребителите в електронния дневник.
13. **Риск:** среден.
14. **ОВЗД:** не, освен при въвеждане на нова платформа с висок риск.

7. Документация, свързана с образователната дейност

1. **Описание:** лични образователни дела, регистрационни книги, удостоверения, протоколи, заявления, справки.
2. **Лица с достъп:** директор, заместник-директори, ЗАС, класни ръководители, учители.
3. **Източник:** ученици, родители, учители, НЕИСПУО, други институции.
4. **Цели:** изпълнение на държавния образователен стандарт за информация и документи.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД; ЗПУО, Наредба № 8/11.08.2016 г. на МОН и приложимите нормативни актове.
6. **Категории данни:** имена, ЕГН, дата на раждане, адрес, родителски данни, оценки, отсъствия, здравни данни при необходимост, ТЕЛК/СОП документи.
7. **Субекти:** ученици, родители.
8. **Получатели:** МОН, РУО, община, НЕИСПУО, други училища при преместване.
9. **Трансфер:** няма.
10. **Срок:** съгласно Наредба № 8, номенклатурата и архивните правила: 3 г., 5 г., 50 г. или постоянно според документа.
11. **Локация:** НЕИСПУО, дирекция, архивохранилище.

12. **Мерки:** заключен архив, ограничен достъп, електронна идентификация.
13. **Риск:** среден; висок при здравни/СОП документи.
14. **ОВЗД:** при нови мащабни електронни системи или систематично обработване на специални категории.

8. Издаване на удостоверения, свидетелства, дипломи и дубликати

1. **Описание:** издаване на документи за завършен клас, етап, степен на образование, професионална квалификация, дубликати.
2. **Лица с достъп:** директор, ЗДУД, ЗАС, оправомощени служители.
3. **Източник:** архивни документи, НЕИСПУО, заявления.
4. **Цели:** удостоверяване на образование и квалификация.
5. **Основание:** чл. 6, пар. 1, т. "В" от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН, както и упражняването на официални правомощия, които са предоставени на администратора (чл. 6, пар. 1, т. "Д" от ОРЗД) (чл. 6, пар. 1, т. "Б" от ОРЗД).
6. **Категории данни:** имена, ЕГН, оценки, завършен клас/степен, професия/специалност, регистрационни номера.
7. **Субекти:** настоящи и бивши ученици.
8. **Получатели:** заявителят, МОН/НЕИСПУО, други органи по закон.
9. **Трансфер:** няма.
10. **Срок:** съгласно Наредба № 8 и архивните правила.
11. **Локация:** дирекция, НЕИСПУО, архив.
12. **Мерки:** проверка на самоличност, ограничен достъп, регистрация на издаването.
13. **Риск:** среден.
14. **ОВЗД:** не.

9. Квалификация на персонала

1. **Описание:** организиране и отчитане на квалификация на педагогически специалисти и служители.
2. **Лица с достъп:** директор, заместник-директори, ЗАС, счетоводител, председател на комисията по квалификация.
3. **Източник:** служители, обучителни организации, МОН/РУО.
4. **Цели:** професионално развитие, изпълнение на нормативни задължения, отчетност.
5. **Основание:** чл. 6, пар. 1, т. "В" от ОРЗД – ЗПУО, Наредба № 15 от 22 юли 2019 г. за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти и приложимите нормативни актове.
6. **Категории данни:** имена, ЕГН при необходимост, длъжност, квалификация, обучения, сертификати, резултати.
7. **Субекти:** служители.

8. **Получатели:** МОН, РУО, обучителни организации, община.
9. **Трансфер:** няма.
10. **Срок:** съгласно номенклатурата и приложимите нормативни актове.
11. **Локация:** дирекция/ТРЗ/архив.
12. **Мерки:** ограничен достъп, съхранение в досие/архив.
13. **Риск:** нисък до среден.
14. **ОВЗД:** не.

10. Прием на ученици

1. **Описание:** кандидатстване, класиране, записване и преместване.
2. **Лица с достъп:** директор, заместник-директор, комисия по прием, ЗАС, длъжностно лице, работещо с електронната деловодна система на училището, оправомощени учители.
3. **Източник:** ученици, родители, предходни училища, НЕИСПУО.
4. **Цели:** прием и записване, администриране на ученически статус, да се получи необходимата информация относно ученика, за да може да се провежда нормално учебния процес и да се поддържа необходимата по закон документация свързана с него.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД; ЗПУО, Наредба № 8/11.08.2016 г. на МОН и други приложими нормативни актове..
6. **Категории данни:** имена, ЕГН, дата на раждане, адрес, родителски данни, оценки, документи за завършен клас/етап, здравни данни при необходимост, данни за общопрактикуващия им лекар, оценки на учениците, здравословното им състояние, имейли, номера на телефони, Решения на ТЕЛК.
7. **Субекти:** кандидати, ученици, родители.
8. **Получатели:** МОН, РУО, община, НЕИСПУО.
9. **Трансфер:** няма.
10. **Срок:** съгласно Наредба № 8/11.08.2016 г и номенклатурата, Книга за подлежащите на задължително обучение до 16 години – 50 години, Дневник – 5 години и Документи за прием след I, II и III класиране -списъци, заявления, тетрадки за завеждане на класирани ученици, Удостоверения за преместване на ученик- срок на съхрание 3 години.
11. **Локация:** дирекция/НЕИСПУО/архив.
12. **Мерки:** ограничен достъп, проверка на документи, архивиране.
13. **Риск:** среден.
14. **ОВЗД:** не.

11. Трудова медицина

1. **Описание:** профилактика, оценка на работоспособност, извършване на необходимите прегледи на работниците/служителите; превенция на заболяванията, здравословни и безопасни условия на труд.
2. **Лица с достъп:** директор, домакин, лице по ЗБУТ, служба по трудова медицина в рамките на необходимото.
3. **Източник:** служители, служба по трудова медицина, медицински специалисти.
4. **Цели:** изпълнение на задължения по ЗБУТ, оценка и превенция на професионални рискове или заболявания.
5. **Основание:** чл. 6, пар. 1, т. "В" от ОРЗД - Закона за здравословни и безопасни условия на труд; чл. 9, пар. 2, б. „б" и „з" ОРЗД.
6. **Категории данни:** имена, ЕГН, длъжност, здравна годност, медицински заключения, ТЕЛК при приложимост.
7. **Субекти:** служители/работници.
8. **Получатели:** служба по трудова медицина, Инспекция по труда, НОИ/компетентни органи при законово основание.
9. **Трансфер:** няма.
10. **Срок:** съгласно ЗБУТ, подзаконовите актове и договора със службата по трудова медицина; в Училището се съхраняват само необходимите заключения/документи за приложимия нормативен срок.
11. **Локация:** ТРЗ/дирекция, отделно от общите досиета при здравни документи.
12. **Мерки:** ограничен достъп, отделно съхранение, поверителност.
13. **Риск:** среден.
14. **ОВЗД:** не, освен при въвеждане на мащабна електронна система.

12. Здравно обслужване на ученици

1. **Описание:** здравно-превантивни дейности, медицински кабинет, здравна информация за ученици.
2. **Лица с достъп:** медицински специалист, директор, ЗДУД, /класен ръководител само при необходимост и в разрешен обем.
3. **Източник:** родители, ученици, медицински документи, общопрактикуващи лекари, компетентни органи.
4. **Цели:** здравна превенция, реакция при инциденти, защита на здравето, изпълнение на задължения по здравното и образователното законодателство.
5. **Основание:** чл. 6, пар. 1, б. „в", „г" и „д" ОРЗД; чл. 9, пар. 2, б. „б", „з" и „и" ОРЗД; Закон за здравето и приложими наредби.
6. **Категории данни:** имена, ЕГН/дата на раждане, клас, здравословно състояние, имунизационни/профилактични данни, алергии, хронични заболявания, контакт при спешност.
7. **Субекти:** ученици.

8. **Получатели:** РЗИ, общопрактикуващи лекари, спешна помощ, родители, компетентни органи при законово основание.
9. **Трансфер:** няма.
10. **Срок:** съгласно приложимите здравни и образователни правила; училището съхранява само необходимата информация за периода на обучение и нормативно изискуемите срокове.
11. **Локация:** медицински кабинет, заключен шкаф/медицинска документация.
12. **Мерки:** отделно съхранение, достъп само за медицински специалист и оправомощени лица при необходимост.
13. **Риск:** висок.
14. **ОВЗД:** преценка при електронна система или мащабно обработване.

13. Служебни бележки, справки и удостоверения за служители

1. **Описание:** издаване на документи за настоящи и бивши служители.
2. **Лица с достъп:** директор, ЗАС, счетоводител, касиер, домакин.
3. **Източник:** трудови и счетоводни документи.
4. **Цели:** удостоверяване на трудов стаж, доход, осигурителни данни и други обстоятелства.
5. **Основание:** чл. 6, пар. 1, б. „в“ ОРЗД; КТ, КСО, данъчно и осигурително законодателство.
6. **Категории данни:** имена, ЕГН, длъжност, стаж, доход, осигурителни данни, банкова/финансова информация при необходимост.
7. **Субекти:** настоящи и бивши служители.
8. **Получатели:** заявителят, НОИ, НАП, банки или други лица само по искане/основание.
9. **Трансфер:** няма.
10. **Срок:** според номенклатурата и документите, от които се черпи информацията.
11. **Локация:** входящ/изходящ регистър, ТРЗ, архив.
12. **Мерки:** проверка на самоличност, ограничен достъп.
13. **Риск:** среден.
14. **ОВЗД:** не.

14. Дарения

1. **Описание:** регистриране на дарения и издаване на свидетелства/документи.
2. **Лица с достъп:** директор, библиотекар, ЗАС, счетоводител, комисия по даренията.
3. **Източник:** дарителят.
4. **Цели:** приемане, отчетност и документиране на дарения.

5. **Основание:** чл. 6, пар. 1, б. „в“ и „б“ ОРЗД; ЗПУО, счетоводно и данъчно законодателство.
6. **Категории данни:** имена, ЕГН/ЛНЧ при необходимост, адрес, контакт, вид и стойност на дарението, подпис.
7. **Субекти:** дарители — физически лица; представители на юридически лица.
8. **Получатели:** община, МОН/РУО, НАП, одитни органи при законово основание.
9. **Трансфер:** няма.
10. **Срок:** съгласно Наредба № 8/11.08.2016 г. на МОН, счетоводни и архивни правила.
11. **Локация:** счетоводство/домакин/архив.
12. **Мерки:** ограничен достъп, счетоводна отчетност.
13. **Риск:** нисък до среден.
14. **ОВЗД:** не.

15. Изпити

1. **Описание:** провеждане на изпити- приравнителни, за промяна на оценка, за определяне на срочна и/или годишна оценка, зрелостни, квалификационни и други изпити.
2. **Лица с достъп:** директор, заместник-директори, комисии, учители, ЗАС.
3. **Източник:** ученици, учители, изпитни комисии, НЕИСПУО.
4. **Цели:** идентификация, провеждане, оценяване и документиране на резултати.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД; ЗПУО, Наредба № 8/11.08.2016 г. на МОН, наредби за оценяване.
6. **Категории данни:** имена, ЕГН/идентификатор, клас, резултат, оценка, протоколи.
7. **Субекти:** ученици, кандидати.
8. **Получатели:** МОН, РУО, НЕИСПУО, комисии, компетентни органи.
9. **Трансфер:** няма.
10. **Срок:** протоколи и документи — съгласно Наредба № 8/11.08.2016 г. на МОН и номенклатурата, често 50 години за документи с удостоверителна стойност (Протокол за резултатите от писмен, устен, приравнителен и поправителен изпит, Протокол на зрелостната комисия за окончателните резултати, Протокол на комисията за придобиване на професионална квалификация за окончателните резултати от държавните квалификационни и зрелостни изпити, Протокол на комисията за удостоверяване на завършено средно образование – срок на съхранение 50 години).
11. **Локация:** кабинет ЗДУД/НЕИСПУО/архив.
12. **Мерки:** псевдонимизация при обявяване на резултати, ограничен достъп.
13. **Риск:** среден.
14. **ОВЗД:** не.

16. Състезания, олимпиади и конкурси

1. **Описание:** участие и класиране в олимпиади, състезания и конкурси.
2. **Лица с достъп:** директор, учители, комисии, ЗАС.
3. **Източник:** ученици, родители, учители.
4. **Цели:** организация, участие, оценяване, класиране, награждаване.
5. **Основание:** чл. 6, пар. 1, б. „в“, „д“ и при незадължителни дейности — „а“ ОРЗД за конкретни публикации/снимки.
6. **Категории данни:** имена, клас, училище, резултат, контакти, снимки само при основание.
7. **Субекти:** ученици.
8. **Получатели:** МОН, РУО, организатори, партньори, жури; публично оповестяване само в минимален обем.
9. **Трансфер:** няма, освен при международни състезания с гаранции.
10. **Срок:** според правилата на състезанието и номенклатурата; публични списъци — само за необходимия срок.
11. **Локация:** дирекция/архив/електронни платформи.
12. **Мерки:** минимизиране, псевдонимизация при възможност.
13. **Риск:** среден.
14. **ОВЗД:** не, освен при международни платформи/мащабно публикуване.

17. Стипендии

1. **Описание:** кандидатстване, класиране и изплащане на стипендии.
2. **Лица с достъп:** директор, комисия, счетоводител, ЗАС, класни ръководители при необходимост.
3. **Източник:** ученици, родители, училищни документи, счетоводство.
4. **Цели:** определяне на право на стипендия и изплащане.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД; ЗПУО, актове на МС/община/МОН.
6. **Категории данни:** имена, ЕГН, клас, успех, доходи/семейно положение при социални стипендии, банкова сметка, родителски данни.
7. **Субекти:** ученици, родители/членове на домакинството при социални критерии.
8. **Получатели:** банки, община, МОН/РУО, одитни органи.
9. **Трансфер:** няма.
10. **Срок:** съгласно счетоводните и архивните срокове.
11. **Локация:** счетоводство/дирекция/архив.
12. **Мерки:** ограничен достъп, минимизиране на публикуваните списъци.
13. **Риск:** среден; висок при социални/здравни основания.

14. **ОВЗД:** преценка при мащабни електронни платформи.

18. Производствени практики, стажове

1. **Описание:** организиране и провеждане на практики/стажове извън Училището.
2. **Лица с достъп:** директор, заместник-директори, ръководители практика.
3. **Източник:** ученици, родители, работодатели/партньори.
4. **Цели:** провеждане на практическо обучение, застраховане, отчетност, комуникация с приемаща организация.
5. **Основание:** чл. 6, пар. 1, б. „в“, „д“ и при договор — „б“ ОРЗД; ЗПУО и нормативни актове за професионалното образование.
6. **Категории данни:** имена, ЕГН/дата на раждане, клас, професия/специалност, контакти, оценка, застрахователни данни, данни за родител при непълнолетни.
7. **Субекти:** ученици, родители.
8. **Получатели:** приемащи работодатели/организации, застрахователи, МОН/РУО.
9. **Трансфер:** няма.
10. **Срок:** съгласно договорите, отчетността и номенклатурата; обичайно до приключване и архивен срок.
11. **Локация:** кабинет ЗДУД/архив/електронна система.
12. **Мерки:** договорни клаузи за поверителност и ограничено използване.
13. **Риск:** среден.
14. **ОВЗД:** не.

19. Национални програми и проекти

1. **Описание:** участие в национални програми, проекти и инициативи.
2. **Лица с достъп:** директор, ЗДУД, счетоводител, ЗАС, ръководители програма, учители.
3. **Източник:** ученици, родители, служители, МОН/РУО/партньори.
4. **Цели:** изпълнение, отчетност, финансиране, участие.
5. **Основание:** чл. 6, пар. 1, б. „в“, „д“ и при договор — „б“ ОРЗД.
6. **Категории данни:** имена, ЕГН/дата на раждане, адрес, контакти, клас/длъжност, банкови данни при плащания, данни за родители при непълнолетни.
7. **Субекти:** ученици, родители, служители.
8. **Получатели:** МОН, РУО, община, ЦРЧР, партньорски организации, одитни органи.
9. **Трансфер:** няма, освен ако програмата не предвижда друго с гаранции.
10. **Срок:** според програмата; обичайно 5 години след приключване, ако не е предвиден друг срок.
11. **Локация:** дирекция/счетоводство/архив.

12. **Мерки:** ограничен достъп, договорни клаузи, минимизиране.
13. **Риск:** среден.
14. **ОВЗД:** преценка според програмата.

20. Библиотека

1. **Описание:** регистрация на читатели и заемане на библиотечни материали.
2. **Лица с достъп:** библиотекар, директор при необходимост.
3. **Източник:** ученици/служители.
4. **Цели:** водене на читателски картон, проследяване на заети книги.
5. **Основание:** чл. 6, пар. 1, б. „д“ и/или „в“ ОРЗД; приложими правила за училищната библиотека.
6. **Категории данни:** имена, клас/длъжност, контакт, заети материали.
7. **Субекти:** ученици, служители.
8. **Получатели:** няма, освен при законово основание.
9. **Трансфер:** няма.
10. **Срок:** до приключване на читателския картон и уреждане на задълженията.
11. **Локация:** библиотека.
12. **Мерки:** ограничен достъп.
13. **Риск:** нисък.
14. **ОВЗД:** не.

21. Обща и допълнителна подкрепа за личностно развитие

1. **Описание:** предоставяне на обща и/или допълнителна подкрепа, работа с екипи, психолог, педагогически съветник, ресурсни учители.
2. **Лица с достъп:** директор, заместник-директори, класен ръководител, психолог, педагогически съветник, ресурсен учител, екип за подкрепа, РЦППО/компетентни структури.
3. **Източник:** ученици, родители, учители, медицински/психологически документи, ТЕЛК/ЕЛК, социални и образователни институции.
4. **Цели:** идентифициране на потребности, планиране и предоставяне на подкрепа, проследяване на резултати, изпълнение на ЗПУО и Наредбата за приобщаващото образование.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД; чл. 9, пар. 2, б. „б“, „г“, „з“ и/или „ж“ според конкретния случай; ЗПУО и Наредба за приобщаващото образование.
6. **Категории данни:** имена, ЕГН, клас, адрес, контакти, данни за родители, образователни затруднения, специални образователни потребности, здравни данни, ТЕЛК/ЕЛК, психологически и педагогически оценки, социална информация.
7. **Субекти:** ученици, родители/настойници.

8. **Получатели:** РЦПППО, МОН/РУО, ДСП/ОЗД, медицински специалисти, община, други органи при законово основание.
9. **Трансфер:** няма.
10. **Срок:** съгласно ЗПУО, Наредба за приобщаващото образование, Наредба № 8/11.08.2016 г. на МОН и номенклатурата; документите се съхраняват само за необходимия нормативен срок.
11. **Локация:** кабинет ОПЛР и ДПЛР/ отделно досие/.
12. **Мерки:** строго ограничен достъп, отделно съхранение, поверителност, минимизиране.
13. **Риск:** висок.
14. **ОВЗД:** преценка; препоръчителна при систематично електронно обработване или обмен с множество институции.

22. Счетоводство

1. **Описание:** счетоводна, данъчна и финансова отчетност.
2. **Лица с достъп:** счетоводител, касиер, директор, одитни органи при проверка.
3. **Източник:** служители, ученици/родители при плащания, контрагенти, банки.
4. **Цели:** плащания, отчетност, бюджет, данъци, осигуровки, одит.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „б“ ОРЗД; Закон за счетоводството, данъчно и осигурително законодателство.
6. **Категории данни:** имена, ЕГН/ЛНЧ при необходимост, адрес, банкова сметка, доходи, плащания, фактури, договори.
7. **Субекти:** служители, ученици/родители, физически лица — контрагенти, представители.
8. **Получатели:** банки, НАП, община, МОН/РУО, одитни органи.
9. **Трансфер:** няма.
10. **Срок:** съгласно Закона за счетоводството, данъчното законодателство и номенклатурата.
11. **Локация:** счетоводство/архив/счетоводен софтуер.
12. **Мерки:** ограничен достъп, пароли, архивиране, заключени шкафове.
13. **Риск:** среден.
14. **ОВЗД:** не.

23. Архив

1. **Описание:** учрежденски архив и съхранение на документи.
2. **Лица с достъп:** ЗАС, архивар/лице, определено със заповед.
3. **Източник:** всички дейности на Училището.

4. **Цели:** архивиране, съхранение, справки, предаване в държавен архив, унищожаване по реда на закона.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД; Закон за Националния архивен фонд и приложими архивни правила, Закона за Националния архивен фонд, чл. 37, 38, 39 и 40 от Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общинските институции.
6. **Категории данни:** всички категории данни, съдържащи се в архивните документи.
7. **Субекти:** ученици, родители, служители, контрагенти, трети лица.
8. **Получатели:** държавен архив, компетентни органи, лица с правен интерес.
9. **Трансфер:** няма.
10. **Срок:** съгласно номенклатурата и архивните правила.
11. **Локация:** архивохранилище.
12. **Мерки:** заключено помещение, регистър за достъп, приемо-предавателни протоколи.
13. **Риск:** среден.
14. **ОВЗД:** не.

24. Входящ регистър

1. **Описание:** регистриране на входящи документи.
2. **Лица с достъп:** ЗАС, домакин, директор, заместник-директори.
3. **Източник:** податели на документи.
4. **Цели:** деловодно администриране.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД; ЗПУО, Наредба № 8/11.08.2016 г. на МОН, деловодни правила.
6. **Категории данни:** имена, адрес/контакт, входящ номер, кратко описание на документа, съдържащите се в документа данни.
7. **Субекти:** податели, лица, за които се отнасят документите.
8. **Получатели:** вътрешни звена, компетентни органи при законово основание.
9. **Трансфер:** няма.
10. **Срок:** съгласно Наредба № 8/11.08.2016 г. на МОН и номенклатурата.
11. **Локация:** канцелария/електронна деловодна система.
12. **Мерки:** ограничен достъп, деловоден ред.
13. **Риск:** нисък до среден.
14. **ОВЗД:** не.

25. Изходящ регистър

1. **Описание:** регистриране на изходящи документи.

2. **Лица с достъп:** ЗАС, домакин, директор, заместник-директори.
3. **Източник:** вътрешни документи, заявления, преписки.
4. **Цели:** деловодно администриране и изпращане на документи.
5. **Основание:** чл. 6, пар. 1, б. „в“ и „д“ ОРЗД, Наредба № 8/11.08.2016 г. на МОН, деловодни правила.
6. **Категории данни:** имена на адресати, адрес/контакт, изходящ номер, кратко описание, съдържащи се в документа данни.
7. **Субекти:** адресати, ученици, родители, служители, трети лица.
8. **Получатели:** адресатите, компетентни органи.
9. **Трансфер:** няма.
10. **Срок:** съгласно Наредба № 8/11.08.2016 г. на МОН и номенклатурата.
11. **Локация:** канцелария/електронна деловодна система.
12. **Мерки:** контрол при изпращане, проверка на адресат, ограничен достъп.
13. **Риск:** нисък до среден.
14. **ОВЗД:** не.

26. Регистър на договорите

1. **Описание:** регистриране и съхранение на договори, различни от трудовите.
2. **Лица с достъп:** директор, ЗДУД, счетоводител, ЗАС.
3. **Източник:** контрагенти, представители, лица за контакт.
4. **Цели:** сключване, изпълнение, отчетност и архивиране на договори.
5. **Основание:** чл. 6, пар. 1, б. „б“ и „в“ ОРЗД; ЗЗД, ЗОП при приложимост, Закон за счетоводството, Наредба № 8/11.08.2016 г. на МОН.
6. **Категории данни:** имена, ЕГН/ЛНЧ при физически лица или ЕТ, адрес, телефон, e-mail, подпис, длъжност на представител, банкова сметка при физически лица. Данни за юридически лица не са лични данни, освен данните за техните представители и лица за контакт.
7. **Субекти:** физически лица — контрагенти, представители, лица за контакт, изпълнители.
8. **Получатели:** банки, НАП, община, МОН/РУО, одитни органи, АОП при приложимост.
9. **Трансфер:** няма.
10. **Срок:** съгласно договорната, счетоводната и архивната номенклатура; обичайно минимум до изтичане на давностни, отчетни и одитни срокове (10 г. (Наредба № 8/11.08.2016 г. на МОН) След изтичане на договора и одит 5 години).
11. **Локация:** дирекция/счетоводство/архив.
12. **Мерки:** заключени шкафове, ограничен достъп, електронна защита.

13. **Риск:** нисък до среден.

14. **ОВЗД:** не.

Приложение № 4

ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ И НЕРАЗПРОСТРАНЕНИЕ НА ЛИЧНИ ДАННИ

Долуподписаният/ата:
.....
Длъжност: .....

ДЕКЛАРИРАМ, ЧЕ:

1. Ще обработвам лични данни само при и по повод изпълнение на служебните ми задължения.
2. Няма да разпространявам, предоставям, публикувам, копирам, изнасям или използвам информация за личните данни на трети лица, станали ми известни при изпълнение на служебните ми задължения и няма да ги използвам за други цели, освен за прякото изпълнение на служебните ми задължения.
3. Запознат/а/ съм със законодателството за защита на личните данни. Ще спазвам Регламент (ЕС) 2016/679, Закона за защита на личните данни, настоящите вътрешни правила и указанията на администратора.
4. Ще пазя поверителността на личните данни и след прекратяване на трудовото/служебното ми отношение.
5. Ще уведомя незабавно директора и ДЛЗД при съмнение за нарушение на сигурността.
6. Нося отговорност за опазване на документите, съдържащи лични данни.
7. Запознат/а съм, че при нарушение нося дисциплинарна, административнонаказателна, гражданска и/или наказателна отговорност.

Дата: ..... г.

Декларатор: .....

Приложение № 5

ИЗВЕСТИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА УЧЕНИЦИ И РОДИТЕЛИ

Администратор: .....
Адрес:.....
Тел.:.....
E-mail: .....

Длъжностно лице по защита на данните: .....
E-mail:.....
Тел.: .....

Относно следните лични данни: лични данни на ученика – егн, имена, адрес, гражданство, месторождение; здравна и медицинска информация (вкл. личен лекар, здравно-профилактични карти, заболявания, наличие на трайни увреждания и др.); информация за специални образователни потребности на лицата; информация за присъствие, отсъствия (причини за отсъствието) и успех (оценяване) на ученика; информация за полагане на изпити (национално външно оценяване, олимпиади, състезания, конкурси и др.); информация за издаване на удостоверения, свидетелства, ученически книжки и ученически лични карти; информация, необходима за предоставяне на награди; данни за родители и деца във връзка с предоставяне на социално подпомагане; данни за родители – име, телефон, ЕГН, месторабота, адрес, e-mail и др.; информация за членовете на обществения съвет – трите имена, адрес, месторабота, телефон, e-mail; информация за получени дарения; фото и видеоматериали, включително снимки на учениците за техни досиета или документи.

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

Попълване на необходимата документация и осъществяване на дейността на училището (например - прием, записване и обучение; водене на задължителна училищна документация; оценяване, изпити и издаване на документи; здравна превенция и спешни реакции; обща/допълнителна подкрепа; стипендии и социални плащания; участие в състезания, олимпиади и проекти; архивиране и отчетност).

Законът изисква от нас да определим въз основа на кое законово основание обработваме различни категории лична информация и да Ви уведомим за основанията и нашите цели, спрямо всяка категория обработвани лични данни.

Ако основанието, на което обработваме Вашата лична информация, вече не е приложимо, ние незабавно ще прекратим обработването на Вашите данни.

Ако основанието се промени, тогава, ако това се изисква от закона, ние ще Ви уведомим за промяната, както и за всяко ново основание, при което сме установили, че можем да продължим да обработваме Вашата информация.

В повечето случаи ние обработваме съответните лични данни на базата на законово задължение, произтичащо от приложимата правна уредба (Закон за предучилищното и училищното образование; НАРЕДБА № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование; НАРЕДБА № 10 от 2017 г. за познавателните книжки, учебниците и учебните помагала; НАРЕДБА за приобщаващото образование; НАРЕДБА за финансирането на институциите в системата на предучилищното и училищното образование; Наредба № 11 от 2016 г. за оценяване на резултатите от обучението на учениците; Наредба № 10 от 2016 г. за организация на дейностите в училищното образование; НАРЕДБА № 3 от 6 април 2017 г. за условията и реда за приемане и обучение на лицата, търсещи или получили международна закрила; НАРЕДБА № 2 от 24.01.2017 г. за регистъра на институциите в системата на предучилищното и училищното образование; НАРЕДБА за детските и ученическите туристически пътувания с обща цена, инициирани от институциите в системата на предучилищното и училищното образование; НАРЕДБА № 15 от 08.12.2016 г. за инспектирането на детските градини и училищата; НАРЕДБА № 13 от 21.09.2016 г. за гражданското, здравното, екологичното и интеркултурното образование; НАРЕДБА № 12 от 01.09.2016 г. за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти; Наредба № 9 от 19 август 2016 г. за институциите в системата на предучилищното и училищното образование; Наредба № 6 от 11 август 2016 г. за усвояването на българския книжовен език; Конвенция за правата на детето; Закон за закрила на детето; Правилник за прилагане на закона за закрила на детето; ПМС № 100 от 08.06.2018 г. за създаване и функциониране на Механизъм за съвместна работа на институциите по обхващане и включване в образователната система на деца и ученици в задължителна предучилищна и училищна възраст).

Записи от системи за видеонаблюдение с охранителна цел - опазване на живота и здравето на учениците и служителите в училището, получени от разположените видеокамери.

Училището декларира, че личните Ви данни ще бъдат третирани като строго поверителни и няма да бъдат споделяни, освен на компетентни органи, институции, доставчици и други получатели при наличие на правно основание, в необходимия минимален обем и при спазване на приложимите мерки за защита.

Ще се съхраняват Вашите лични данни не повече от предвидените в закона срокове: личните данни в личните картони/личните образователни дела на учениците се пазят 50 години, в дневниците - 5 години, Книга за подлежащите на задължително обучение до 16 години – 50 години, като данните ще бъдат съхранявани по следния начин: всички документи, съдържащи лични данни, се съхраняват при необходимите технически и организационни мерки за защита.

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

- имате право да поискате копие от Вашите лични данни и право на достъп по всяко време до личните си данни; имате право да прехвърлите личните си данни на друг администратор на лични данни, без да бъдете възпрепятствани от наша страна при налична такава законова възможност;

- имате право да поискате да се коригират без ненужно забавяне неточните Ви лични данни, както и данните, които не са вече актуални. За целите на коригиране или допълване на

личните Ви данни трябва да подадете отделна декларация, в която да посочите актуални лични данни;

- имате право да поискате от администратора личните Ви данни да бъдат изтрити без ненужно забавяне при наличието на някое от следните основания: личните данни повече не са необходими за целите, за които са били събрани; когато сте оттеглил своето съгласие; когато сте възразил срещу обработването, когато обработването е незаконосъобразно; когато личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на ЕС или правото на държава членка, което се прилага спрямо администратора; когато личните данни са били събрани във връзка с предлагането на услуги на информационното общество. Администраторът може да откаже да заличи личните данни по следните причини: упражняване на правото на свобода на изразяването и правото на информация; за спазване на правно задължение от администратора или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратора; по причини от обществен интерес и в областта на общественото здраве; за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото съществува вероятност заличаването да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или за установяването, упражняването или защитата на правни претенции.

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

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

Долуподписаният ..... с подписването потвърждавам, че съм прочел това известие за защита на данните, като съм получил разяснение на зададените от мен въпроси във връзка с личните данни.

Разбирам напълно описаното в настоящото известие и ще се възползвам от предоставените ми права при необходимост.

Декларирам истинността на посочените от мен лични данни. За неверни данни нося наказателна отговорност.

Дата…….. Подпис на родител:……..

Приложение № 6

ИЗВЕСТИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА СЛУЖИТЕЛИ И КАНДИДАТИ ЗА РАБОТА

Администратор: .....
Адрес:.....
Тел.:.....
E-mail: .....

Длъжностно лице по защита на данните: .....
E-mail:.....
Тел.: .....

Относно следните лични данни: име, ЕГН, номер и дата на издаване на лична карта, адрес, семейно положение и деца (в определени случаи: лични данни на съпруг/съпруга и други близки за упражняване на трудови права, напр. при отпуск по майчинство), информация за трудовия стаж и професионалния Ви опит (включително заемани длъжности, работно време, стаж по специалността), информация за банкови сметки, заплата и социални придобивки, месторабота, информация за подбор (включително копия от разрешителни за работа, препоръки и друга информация, посочена във Вашата автобиография и придружително писмо или предоставена по друг начин чрез процеса на кандидатстване, информация относно трудова дисциплина, получени от Вас при сключването на трудовия договор или впоследствие при изпълняването му и на произхождащото от него трудово правоотношение.

В качеството си на администратор на лични данни и изпълнявайки задълженията си съгласно Общия регламент за защита на данните декларирам, че ще използвам Вашите лични данни, описани по-горе, за следната цел: сключване, изпълнение и прекратяване на трудовия договор и произхождащото от него трудово правоотношение.

Основание за обработването: сключване на трудовия договор и произхождащото от него трудово правоотношение, както и законовите задължения, предвидени в Кодекса на труда и всички други приложими нормативни актове.

Записи от системи за видеонаблюдение с охранителна цел - опазване на живота и здравето на служителите и учениците, сред които има и деца, в училището, получени от разположените видеокамери.

Ще бъдат обработвани и следните специални категории по-чувствителни данни за Вас:

- Членство в синдикални организации, получени от Вас и от синдикалната организация с цел да се ползвате от правата си при членуване в такава организация.

- Информация за Вашето здравословно състояние, получена от Вас при евентуално представяне от Ваша страна на болничен лист или решение на ТЕЛК, с цел да се изпълнят предвидените в закона права и задължения.

- Информация за наказателни присъди и нарушения, получени от Вас чрез задължително подадена декларация и получена от нас информация от съда, тъй като това е предвидено задължение в закона.

Декларирам, че личните Ви данни ще бъдат третирани като строго поверителни и няма да бъдат споделяни, освен на компетентни органи, институции, доставчици и други получатели при наличие на правно основание, в необходимия минимален обем и при спазване на приложимите мерки за защита.

Ще съхранявам Вашите лични данни не повече от предвидените в закона срокове, за трудовото правоотношение – трудово досие 5 години след напускане или пенсиониране на служителя, ведомости за заплати – 50 години, болнични листове - 3 години след одит, видеонаблюдение – 6 месеца, като всички документи, съдържащи лични данни, се съхраняват при необходимите технически и организационни мерки за защита.

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

- имате право да поискате копие от Вашите лични данни и право на достъп по всяко време до личните си данни;

- имате право да прехвърлите личните си данни на друг администратор на лични данни, без да бъдете възпрепятствани от наша страна при налична такава законова възможност;

- имате право да поискате да коригирам без ненужно забавяне неточните Ви лични данни, както и данните, които не са вече актуални. За целите на коригиране или допълване на личните Ви данни трябва да подадете отделна декларация, в която да посочите актуални лични данни;

- имате право да поискате от администратора личните Ви данни да бъдат изтрити без ненужно забавяне при наличието на някое от следните основания: личните данни повече не са необходими за целите, за които са били събрани; когато сте оттеглил своето съгласие; когато сте възразил срещу обработването, когато обработването е незаконосъобразно; когато личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на ЕС или правото на държава членка, което се прилага спрямо администратора; когато личните данни са били събрани във връзка с предлагането на услуги на информационното общество.

- Администраторът може да откаже да заличи личните данни по следните причини:

1. упражняване на правото на свобода на изразяването и правото на информация;

2. за спазване на правно задължение от администратора или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратор;

3. по причини от обществен интерес в областта на общественото здраве;

4. за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото съществува вероятност заличаването да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или за установяването, упражняването или защитата на правни претенции.

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

- имате право да оттеглите Вашето съгласие за обработване на личните Ви данни по всяко време с отделна молба, депозирана пред администратора в случаите, когато обработването се осъществява въз основа на дадено от Вас съгласие;

- имате право на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисията за защита на личните данни, която е надзорен орган в Република България;

- при нужда Вашите лични данни ще бъдат използвани за нова цел, която не е обхванатата от настоящото известие за защита на данните, ще Ви се предостави ново известие за защита на данните, когато и където е необходимо, ще изискаме Вашето предварително съгласие за новото обработване.

Долуподписаният ..... с подписването потвърждавам, че съм прочел това известие за защита на данните, като съм получил разяснение на зададените от мен въпроси във връзка с личните данни.

Разбирам напълно описаното в настоящото известие и ще се възползвам от предоставените ми права при необходимост.

Декларирам истинността на посочените от мен лични данни. За неверни данни нося наказателна отговорност.

Дата…….. Подпис……

Приложение № 7

ИСКАНЕ ЗА ИЗТРИВАНЕ НА ЛИЧНИ ДАННИ

До Директора на .....

От:.....
ЕГН/ЛНЧ:.....
Адрес/e-mail: .....

Моля да бъдат изтрити следните мои лични данни:

.....
.....

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

Основание за искането:

☐ данните вече не са необходими

☐ оттеглям съгласието си

☐ възразявам срещу обработването

☐ обработването е незаконосъобразно

☐ друго: .....

Известно ми е, че изтриване може да бъде отказано, когато съхранението е необходимо за изпълнение на законово задължение, обществен интерес, архивиране или защита на правни претенции.

Дата: ..... г.

Подпис: .....

Приложение № 8

ВЪЗРАЖЕНИЕ СРЕЩУ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

До Директора на .....

От:.....
ЕГН/ЛНЧ:.....
Адрес/e-mail: .....

Възразявам срещу обработването на следните мои лични данни:

.....
.....

Причини за възражението:

.....
.....

Дата: ..... г.

Подпис: .....

Приложение № 9

ПРОТОКОЛ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Дата и час на установяване: .....

Лице, установило нарушението: .....

На кого е докладвано: .....

Описание на нарушението:

.....
.....

Категории засегнати данни:

.....
.....

Категории и приблизителен брой засегнати лица:

.....
.....

Вероятни последици:

.....
.....

Предприети незабавни мерки:

.....
.....

Оценка на риска:

☐ няма вероятност за риск ☐ риск ☐ висок риск

Уведомяване на КЗЛД:

☐ да ☐ не

Мотиви:
.....
.....

Уведомяване на субектите:

☐ да ☐ не

Мотиви: .....

ДЛЗД:.....
Директор: .....