Детска градина „Радост”
5400, гр.Севлиево, ул.”Здравец” №1; тел. 0675/ 3-28-46; 8-90-02
info-701351@edu.mon.bg; сайт: www.dg-radost.org

ПОЛИТИКА ЗА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА

Въведение

Настоящата политика е разработена въз основа на насоките в Общия регламент за защита на личните данни, съгласно който защитата на правата и свободите на физическите лица с оглед на обработването на лични данни изисква приемане на подходящи технически и организационни мерки (ТОМ), за да се гарантира изпълнението на изискванията на Общия регламент за защита на личните данни.

Раздел I. Основни принципи

1. За всяка конкретна обработка институцията осигурява подходящи технически и организационни мерки за защита на личните данни, отчитайки:
   1.1. Достиженията на техническия прогрес.
   1.2. Разходите за прилагане на мерките.
   1.3. Естеството на обработването.
   1.4. Обхвата на обработването.
   1.5. Контекста и целите на обработването.
   1.6. Възможните рискове за правата и свободите на физическите лица.
   1.7. Рискове от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.
2. Основен принцип, който институцията спазва, е да не се обработват повече от необходимите лични данни, като това се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност.
3. Данните следва да се обработват само от лицата, обработващи тези данни по указание на администратора.
4. Процесът по обработката следва да бъде документиран.

Раздел II. Насоки за изграждане на система от технически и организационни мерки (ТОМ) за защита на личните данни

5. С оглед на важното значение на ТОМ по отношение на налаганите глоби от надзорния орган, институцията следва да реализира мерки, които се основават на:
   5.1. обучение на служителите, обработващи лични данни;
   5.2. документална обезпеченост на процесите, включително документиране на самите процеси;
   5.3. мониторинг на обработването на данни за своевременно откриване на пробиви в сигурността;

5.4. залагане на изискванията на ОРЗД в нормалните дейности на институцията (избор на доставчици, използване на информационни системи и т.н.).

Раздел III. Приложимо ниво на риск

6. С оглед на множеството паралелни дейности, които се извършват в институцията, тя възприема единна оценка на риска на всички свои дейности, прилагайки най-високия, установен такъв.
7. До наличието на официална национална методология за определяне нивото на риска, институцията приема, че нивото на риск на обработването на данни като администратор се приема за „**ниско**“ – неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.
8. В случай, че институцията е обработващ данни, съответните технически и организационни мерки се определят в договора със съответния администратор или нормативен акт, който регулира това отношение. Институцията си запазва правото самостоятелно да въведе допълнителни мерки за сигурност, които смята за необходими.

Раздел IV. Технически и организационни мерки за защита на личните данни

9. Мерките, посочени по-долу, се основават на възприетото ниво на риск в т.7.
10. Не всички мерки е възможно да се отнасят към обичайната дейност на институцията, но е възможно необходимостта от тях да възникне при дейността на обработващите за институцията данни от трети страни или такива, които създават специфични решения за нея.
11. Техническите и организационни мерки се прилагат, доколкото се поддържа от функционалността на съответното устройство или операционна система, и се използват от институцията във връзка с осъществяването на съответния процес.
12. Мерки, насочени към документалното и оперативното изпълнение на мерките за защита на личните данни:
    12.1. Налична е политика за защита на личните данни;
    12.2. Налична е процедура за действие при нарушение на личните данни;
    12.3. Описание на техническите и организационните мерки по отношение на защита на лични данни.
    12.4. Субсидиарно се прилагат и:
        12.4.1. Политика за информационна сигурност;
        12.4.2. План за непрекъсваемост на работните процеси.
13. Мерки, насочени към служителите:
    13.1. Информиране и засилване на чувствителността на служителите по отношение на обработването на лични данни, включително чрез провеждането на начални обучения;
    13.2. Налагане на задължителна инструкция за допустимата употреба на компютърни устройства на институцията включително налагане на дисциплинарни наказания при нейното нарушаване;
    13.3. Служителите биват информирани и подписват декларация за поверителност.
14. Мерки, насочени към достъпване на информационните системи на институцията.

14.1. Всеки потребител има свой уникален акаунт, който следва да не споделя с никой друг;

14.2. Налице е политика за сложност на паролите за достъп до акаунта, обхващаща всички устройства на институцията (вкл. смартфони, таблети, лаптопи, стационарни компютри, сървъри и т.н.);

14.3. Потребителите следва да променят редовно своята парола, по възможност наложено от самите електронни системи;

14.4. Неуспешните опити за достъп до акаунтите следва да бъде ограничен;

15. Мерки насочени към управление на даването на достъпи до информационните системи на институцията.

15.1. Потребителите имат различни акаунти (профили) за отделните задачи, които извършват;

15.2. Всички ненужни права (например вследствие на напускане или преместване) следва да се премахват своевременно;

15.3. Всички стари права подлежат на редовен преглед и премахване при необходимост поне веднъж в годината;

16. Мерки насочени към сигурността на работните станции.

16.1. Използване само на лицензиран софтуер;

16.2. Регулярно обновяване на антивирусните софтуери;

16.3. Инсталирана софтуерна стена;

16.4. Забрана за инсталиране на неоторизиран софтуер;

16.5. Ограничаване използването на преносима памет;

16.6. Процедури за автоматично заключване на сесиите;

16.7. Редовно инсталиране на критични обновявания;

16.8. Ограничаване използването на Интернет, а ако е невъзможно - използване на софтуери за филтриране на уеб страници и определени действия;

16.9. Използване на стандартните опции за криптиране на дисковете за съхранение на информация на операционните системи;

16.10. Взимане на съгласие преди интервенция от страна на администратора върху работната машина на потребителя.

17. Мерки насочени към сигурността на използваните мобилни устройства.

17.1. Криптиране на мобилните устройства;

17.2. Възможност за отдалечено проследяване на откраднато/загубено устройство;

17.3. Регулярно създаване на резервни копия и синхронизация на данните;

17.4. Смартфоните изискват отключване посредством определено действие, свързано със сигурността.

18. Мерки, насочени към сигурността на вътрешната компютърна мрежа.

18.1. Ограничаване мрежовите потоци само до най-необходимото;

18.2. Осигуряване на достъп на мобилните изчислителни устройства посредством VPN;

18.3. Отделяне на Wi-Fi мрежата от другите мрежи;

18.4. Провеждане на ежегодни тестове за проникване (външни).

19. Мерки, насочени към сигурността на сървърите.

19.1. Ограничаване на достъпа до административни инструменти само за оторизирани лица;

19.2. Незабавна инсталация на критични обновявания;
19.3. Осигуряване на наличността на данните;
19.4. Мерки насочени към сигурността на уеб страниците/уеб системи на институцията;
19.5. Основните данни, които могат да послужат за разпознаване, са криптирани;
19.6. Поставяне на банер за съгласие за бисквитките, които не са необходими за предоставяне на основните услуги.

20. Мерки, насочени към осигуряване на непрекъсваемостта на организационните процеси.
20.1. Създаване на регулярни резервни копия;
20.2. Съхранение на резервните копия на сигурно място;
20.3. Планират се мерки за сигурност за предаване на резервните копия;
20.4. Планиране и тестване на непрекъсваемостта на организационните процеси.

21. Мерки, насочени към осигуряване на сигурността на архивирането.
21.1. Прилагане на специфични процедури за достъп до архивираните данни;
21.2. Унищожаване на старите архиви по сигурен начин.

22. Мерки, насочени към осигуряване на мониторинг върху унищожаването на носители на данни.
22.1. Записване на възможните интервенции в регистър;
22.2. Наблюдаване на интервенциите на трети страни от официално лице на институцията;
22.3. Изтриване на данните от носителя преди неговото унищожаване.

23. Мерки, насочени към контрол на доставчиците.
23.1. Специални клаузи в договорите с доставчиците;
23.2. Предвидени условия за връщане или унищожаване на данните;
23.3. Контрол върху ефективността на предоставените гаранции (одити по сигурността, визити и т.н.).

24. Мерки, насочени към сигурността на обмен на данни с трети страни.
24.1. Изрична проверка, че е подаден верният получател;
24.2. Използване само на служебни електронни пощи, когато съобщението се изпраща по имейл.

25. Мерки, насочени към физическата защита на помещенията
25.1. Ограничаване на достъпа до помещенията посредством заключени врати;
25.2. Инсталиране на аларма против взлом и периодичната им проверка;
25.3. Използване на заключващи шкафове или каси за съхраняване на личните данни и/или преносимите изчислителни устройства;
25.4. Следване на политика на „чисто бюро“.

26. Мерки, насочени към разработчици на електронни системи за институцията.
26.1. Тестването на електронни системи се извършва само с фиктивни или анонимизирани данни;
26.2. В случай на наличието на опционалности, насочени към поверителността на информацията, предлагане на настройки за тях на крайния потребител.

27. Мерки, в случай на необходимост от използване на криптографски услуги.
27.1. Използване на признати алгоритми, софтуери и библиотеки;

Раздел V. Трети страни, обработващи данни

28. В случай на използване на трети страни като обработващи данни, институцията използва само такива обработващи, които предоставят достатъчни гаранции, че ще прилагат подходящи технически и организационни мерки за защита на личните данни. Тези мерки следва да бъдат сходни по обхват на тези, които са определени в раздел „Технически и организационни мерки за защита на личните данни“ от тази политика. Обработването се възлага чрез договор, в който изрично са посочени поне:
    28.1. Предмет на обработването;
    28.2. Срок на обработването;
    28.3. Естеството и целта на обработването;
    28.4. Вида лични данни;
    28.5. Категориите субекти на данни;
    28.6. Задълженията и правата на администратора;
    28.7. Необходимостта от писмено разрешение от страна на институцията за използване на други обработващи от обработващия данни;
    28.8. Обработващият действа само по указания на администратора;
    28.9. Обработващият гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;
    28.10. Обработващият подпомага администратора с всички подходящи средства, за да се гарантира спазването на разпоредбите относно правата на субекта на данни.

Раздел VI. Обновяване на техническите и организационните мерки (ТОМ)

29. За целта на поддържане на ТОМ в актуално състояние с оглед на условията посочени в т.1.1-1.7, всяка година СЗД/ДЛЗД извършва преглед и при необходимост координира необходимостта от промени със засегнатите звена в институцията.

Директор: .....

Цанка Нейчева

Детска градина „Радост”
5400, гр.Севлиево, ул.”Здравец” №1; тел. 0675/ 3-28-46; 8-90-02
info-701351@edu.mon.bg; сайт: www.dg-radost.org

Инструкция за използването на информационите системи от служителите

Раздел I. Общи положения

Чл. 1. (1) Инструкцията за използване на информационните системи информира педагогическите специалисти и непедагогическия персонал за правата и задълженията им по отношение на използването нейното приложение и използване.

(2) Инструкцията определя правилата за използване на информацията за вътрешна и външна комуникация, за предоставяне на услуги на родители и учители, за администриране, свързано с учебно-възпитателния процес, а също така е средство за извършване на проучвания и обмяна на информация.

(3) Достъпът до данните в локалната мрежа и ползването на програмните продукти на институцията от педагогическите специалисти и непедагогическия персонал е необходимо с оглед ефективното изпълнение на отговорностите и задълженията.

Чл. 2. Информационните технологии включват локалните мрежи, интернет, електронната поща и всички програмни продукти, които институцията притежава и ползва.

Чл. 3. Инструкцията дава указания за начина на употреба от педагогическите специалисти и непедагогическия персонал на информационните технологии, насърчава ползването им с цел увеличаване на продуктивността и ефективността на работата.

Чл. 4. (1) ЗАС /компютърен специалист по договор/ в институцията са отговорни за цялостната дейност на информационните технологии и за подпомагането работата на служителите на институцията с тях.

(2) При съмнение за нарушение на сигурността на личните данни, лицето, което е установило несъответствието (случайно или неправомерно унищожаване на лични данни, загуба, промяна, неразрешено разкриване или нерегламентиран достъп, незабавно уведомява лицата по ал. 1 и определения служител по защита на личните данни за предприемане на действия по прилагане на Инструкцията за действие при пробив в сигурността.

Чл. 5. Служителите в институцията са задължени да спазват правилата, определени с настоящата Инструкция.

Чл. 6. Всички компютърни програмни продукти и информация, създадена и съхранена от служителите, са собственост на институцията.

Чл. 7. Служителите в институцията нямат право да вземат програмните продукти с цел инсталирането им на домашните им компютри и преносими устройства, с изключение на електронните познавателни книжки и създадените за

он-лайн обучение софтуери.

Чл. 8. При напускане на институцията служителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

Раздел II. Контрол върху работата с информационните технологии

Чл. 9. (1) Ръководството на институцията има право да контролира ползването на програмните продукти, електронната поща, Интернет и базите данни, създадени от служителите в институцията.

(2) Ръководството на институцията, включително и определеното длъжностно лице по защита на личните данни - ЗАС, имат право да проверява изцяло служебните компютри, предоставени за учебни цели на служителите в институцията, както и техниката, която ползват учители и служители във връзка с изпълнение на служебните им задължения.

Раздел III. Конфиденциалност

Чл. 10. Резултатите от извършения контрол върху работата с информационните технологии на институцията се считат за конфиденциални и не се разгласяват от ръководството.

Раздел IV. Допустимо ползване на информационните технологии за лични цели

Чл. 11. Учебните информационни системи са предназначени за ползване при изпълняване на служебните задължения на служителите.

Чл. 12. Тези системи могат да се ползват и за лични цели при следните условия:

1. Това е инцидентно, рядко и за кратко време.
2. Не е по време на работа, а е в извънработно време.
3. Това не пречи на работата на останалите служители. В това число се включват дейности, които могат да доведат до конфликт на интереси.
4. Това не води до допълнителни разходи за институцията.

Раздел V. Забрани за ползване на информационните технологии

Чл. 13. Забранява се ползването на компютърните и информационните системи на институцията в следните случаи:

1. Заобикаляне на системите за сигурност, с цел разрушаване или намаляване сигурността на учебната локална мрежа или бази данни.
2. Ползване на информационните ресурси за извършване на нерегламентирана дейност.
3. Използване на ресурсите за подпомагане дейността на външни организации, техните продукти, услуги или бизнес практика, с цел облага.
4. Електронна поща на институцията не може да се ползва за комерсиални лични цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на институцията.
5. Ползването на компютърните системи за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат.
6. Подправяне на електронна поща с цел скриване на самоличността на

подателя или фалшифициране на тази самоличност. Всички електронни писма, пращани от служители на институцията трябва да са лично подписани и да са до точно определен брой адресати, които са дали съгласие за използване на електрлонния им адрес.

7. Свалянето от Интернет на аудио и видео файлове и други.
8. Сваляне и инсталиране на компютърни програми от Интернет без разрешение на компютърните специалисти.
9. Копиране на лицензираните компютърни програми на институцията с цел лична употреба.

Раздел VI. Разкриване на информация

Чл. 14. (1) Неоторизираното разкриване на служебна информация може да доведе до негативни последици за институцията и накърняване на нейния имидж и репутация.

(2) Служител, който е копирал и използвал информация от локалната мрежа на институцията за лична изгода или за да причини вреда на институцията, носи съответната дисциплинарна и имуществена отговорност по КТ.

Раздел VII. Антивирусна защита

Чл. 15. (1) Компютърните вируси са голяма заплаха за всички потребители на IT услуги и служителите трябва да имат необходимите знания как вирусите се разпространяват, каква вреда могат да нанесат и как да се предпазват от тях.

(2) Компютърният вирус е компютърна програма, която се задейства на даден компютър и се разпространява към другите дискове и програми, които са в контакт със заразения компютър.

(3) Вирусът може да причини блокиране на компютъра, да промени бази данни, да направи някои данни невъзможни за ползване и даже да форматира диск и така да се загуби цялата информация на тях.

Раздел VIII. Организация на защитата от вируси

Чл. 16. (1) IT специалиста на институцията с които ДГ има догтовор, носи пълната отговорност за избирането и инсталирането на антивирусната програма, както и за нейната актуализация на всеки индивидуален компютър. Служителите също трябва да следят дали тяхната антивирусна програма се осъвременява поне веднъж седмично с най-новата версия.

(2) Служителите трябва да приемат всяко съобщение за вирус изключително сериозно и да следват вътрешните процедури за реакция в такъв случай.

(3) Преднамереното разпространяване на данни, за които служителят знае, че са заразени е нарушение на служебните задължения, което се санкционира по дисциплинарен ред.

(4) В случай на вирусна атака служителят трябва незабавно да информира IT специалист без да предприема никакви действия самостоятелно.

(5) На служителите е разрешено да свалят файлове от външни източници на мрежата на институцията във връзка с тяхната работа. Не е разрешено на служителите да се инсталират програмни продукти без предварителното разрешение на IT специалиста, тъй като има опасност от заразяване с вируси.

(6) Входящата електронна поща трябва да се третира с особено внимание

поради потенциалната възможност да е заразена с вируси. Отварянето на приложения да се прави само след предварителното им сканиране с антивирусна програма.

(7) Електронни писма, получени от неизвестни податели трябва да се изтриват и в никакъв случай да не се отварят файлове, прикачени към тях.

(8) Файлове, получени от неизвестни податели трябва да се трият без да се отварят.

(9) Ползването на външни носители (дискове, външна памет и др.) на информация е допустимо само след предварителното им сканиране с антивирусна програма.

Раздел IX. Архивиране на информацията

Чл. 17. (1) Сривовете в компютърното оборудване, вирусите, случайното изтриване на файлове могат да причинят загуба на данни, поради което е необходимо информацията във всяка компютърна система да бъде архивирана.

(2) Целта на архивирането и възстановяването е да се възстанови работата възможно най-бързо в случай на прекъсване по технически причини. По този начин се минимизират възможните проблеми и загуби.

(3) Служителите в институцията, съгласувайки със ДЛЗЛД, трябва да имат адекватна система за архивиране на данните от своята работа на технически носители (дискове, USB и др.).

(4) Честотата на архивирането се определя от директора в писмена процедура и зависи от броя транзакции и тяхната значимост за системата.

(5) Задължително архив (архивиране на файлове) се прави веднъж месечно.

Раздел X. Достъп и пароли

Чл. 18. (1) Служителите получават достъп до локалната мрежа и до всички програми, необходими за изпълнение на служебните им задължения.

(2) Достъпът до дадена програма се дава на конкретен служител и не може да се прехвърля на друг.

(3) Служителите трябва да пазят своите лични пароли в тайна.

Чл. 19. Когато даден продукт изисква парола трябва да спазват следните правила:

1. служителите трябва да променят първоначалната парола (обикновено генерирана от програмния продукт) като измислят своя индивидуална при първото влизане в съответната информационна система;
2. паролите трябва да са с не по-малко от 5 знака;
3. паролите трябва лесно да се помнят, за да не се налага да бъдат записвани на хартия;
4. паролите не трябва да са лесни за отгатване от колегите;
5. паролите не трябва да се споделят с колеги или други познат;
6. паролите не трябва да се записват на хартия и да се оставят на работното място;
7. ако е необходимо паролите могат да се сменят на определена честота (всеки 3, 6, 12 месеца);
8. при 3 неуспешни опита за влизане в дадена програма достъпът може да бъде блокиран;

9. при периодична промяна на паролата не трябва да се използват вече използвани пароли;
10. системите не трябва да позволяват един и същи потребител да се включи в няколко компютъра едновременно с една и съща парола.

Чл. 20. Ако забравят своята парола служителите трябва незабавно да уведомят оторизирания помощник директор и да се свържат с IT специалист.

Раздел XI. Интернет

Чл. 21. (1) Ръководството насърчава ползването на Интернет от служителите за обмяна на информация, извършване на проучвания и събиране на данни във връзка с дейността им.

(2) ЗАС и други оторизирани длъжностни лица отговарят за уместната употреба на Интернет от служителите на институцията.

(3) Свалянето от Интернет на аудио или видео файлове е забранено. Не е разрешено и свалянето на програмни продукти от Интернет без предварителното одобрение на компютърен специалист.

Раздел XII. Електронна поща

Чл. 22. (1) Електронната поща на институцията не може да се ползва за комерсиални цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на институцията.

(2) Ползването на електронната поща за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат също не се позволява.

(3) Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност се забранява. Всички електронни писма, изпращани от служителите трябва да са лично подписани.

(4) Неформалните съобщения, които не са от официален характер трябва да се трият от пощата, за да не се товарят сървърите на институцията.

(5) Всички електронни писма и важни съобщения, които имат отношение към дейността на училището, трябва да се принтират и представят за завеждане с входящ номер в дневника за входяща кореспонденция от определеното длъжностно лице, като екземпляр се съхранява в съответние класьор и в електронната поща.

(6) Служителите трябва да проверяват внимателно точния адрес на получателите на официални писма, особено такива с прикачени файлове, за да не се допусне получаване на информация от чужди лица.

Раздел XIII. Лице за контакт

Чл. 23. Всички технически въпроси във връзка с работата на компютърните системи се насочват към IT специалистиа на институцията с които образователната институция има договор или към друго лице, определено от директора.

Допълнителни разпоредби

§ 1. При извършване на самооценката на вътрешните контроли следва да се направи анализ и оценка на риска на критичните информационни системи в институцията.

§ 2. Целта е да е идентифицират най-важните компоненти (оборудване, програми, бази данни), заплахата за тяхната повреда или загуба, последиците от това за дейността на институцията налични контроли за да се предотвратят потенциалните проблеми и допълнителни контроли, които са необходими за подобряване на системата.

§ 3. Оценката на риска обхваща извършеното, както и моментното състояние, мерките за подобряване на слабите места във вътрешните контроли, необходимите ресурси и остатъчния риск за институцията, който контролите няма как да елиминират.

§ 4. При създаването на програмен продукт специално за нуждите на институцията е необходимо още при задаването на неговите параметри на доставчика да се заложат основните контролни функции, които този продукт трябва да има.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Инструкцията влиза в сила утвърждаването ѝ със Заповед № РД-09-324/08.03.2024 г. на директора.

Директор: .....
Цанка Ненчева

Детска градина „Радост”
ПК 5400, гр.Севлиево, ул.”Здравец” №1; тел. 0675/ 3-28-46; 8-90-02
info-701351@edu.mon.bg; сайт: www.dg-radost.org

З А П О В Е Д
№ РД-09-323
гр. Севлиево, 08.03.2024 г.

На основание чл. 259, ал. 1 от Закона за предучилищното и училищното образование, чл. 19, ал. 2, т. 14 от Наредба № 12/01.09.2016 г. за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти и във връзка с чл. 7, ал. 1, т. 12 и чл. 14, т. 4 и т. 5 и от Закона за финансовото управление и контрол в публичния сектор и във връзка с необходимостта от постигане на съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица при обработването на лични данни

УТВЪРЖДАВАМ:

1. Вътрешни правила за ползване на информационите системи от служителите.

I. НАРЕЖДАМ:

2. В срок от десет работни дни от издаване на настоящата заповед:
   2.1. утвърдените Вътрешни правила по т. 1 да се доведе до знанието на всички служители в институцията за сведение и изпълнение, което се удостоверява лично с подпис;
   2.2. за запознаването с Вътрешните правила да се създаде списък, съобразно разпоредбите в тях;
   2.3. списъкът по предходната точка да се предаде за съхранение на Виолета Монева - ДЛЗЛД в срок постоянен г.
3. Изпълнението по т. 2 възлагам на Виолета Монева – ДЛЗЛД. За неизпълнение на разпоредбите на Вътрешните правила, виновните лица носят дисциплинарна отговорност.
4. Контролът по изпълнението на заповедта ще упражнявам лично.

ЦАНКА НЕНЧЕВА
Директор на ДГ ”Радост” – Севлиево

Детска градина „Радост”
ПК 5400, гр.Севлиево, ул.”Здравец” №1; тел. 0675/ 3-28-46; 8-90-02
info-701351@edu.mon.bg; сайт: www.dg-radost.org

З А П О В Е Д
№ РД-09-324
гр. Севлиево, 08.03.2024 г.

На основание чл. 259, ал. 1 от Закона за предучилищното и училищното образование и чл. 23, ал. 4 от Закона за защита на личните данни относно необходимостта от защитата на физическите лица при обработването на лични данни във връзка с постигането на съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г.

УТВЪРЖДАВАМ:

1. Политика за технически и организационни мерки за защита на личните данни.
2. Длъжностна характеристика на длъжностно лице по защита на личните данни

НАРЕЖДАМ:

2. В срок от десет работни дни от издаване на настоящата заповед утвърдената Политика за технически и организационни мерки за защита на личните данни да се качи на сайта на образователната институция и да се доведе до знанието на всички служители в институцията за сведение и изпълнение, което се удостоверява лично с подпис.

3. Изпълнението по т. 2 възлагам на Виолета Монева - длъжностното лице по защита на данните.

4. За неизпълнение на разпоредбите на утвърдената Политика за технически и организационни мерки за защита на личните данни, виновните лица носят дисциплинарна отговорност.

Контролът по изпълнението на заповедта ще изпълнявам лично.

ЦАНКА НЕНЧЕВА
Директор на ДГ ”Радост” – Севлиево