СРЕДНО УЧИЛИЩЕ“ХРИСТО БОТЕВ“ С. ГАБАРЕ

общ. Бяла Слатина , ул. “Тома Николов” №1 ***тел.: 09140 44 41;***
Директор: **0897 930 415;** ***e-mail:*** **su_gabare@abv.bg ; http://su-gabare.org/**

УТВЪРЖДАВАМ:
ИНЖ. МАРИО НИКОЛОВ
ДИРЕКТОР НА СУ „ХРИСТО БОТЕВ“ С. ГАБАРЕ

Заповед № 721/14.09.2020 г.

ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ НА СУ „ХРИСТО БОТЕВ” С. ГАБАРЕ

ГЛАВА ПЪРВА
I.ВЪВЕДЕНИЕ

Чл. 1. (1) С тези вътрешни правила се уреждат редът и условията за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни, както и мерките и средствата за тяхната защита.
(2) Настоящите правила се издават на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД).
(3) Правилата се утвърждават, допълват, изменят и отменят от Директора на СУ „Христо Ботев” с. Габаре – администратор на лични данни.
(4) Администраторът предоставя достъп до обработваните от него лични данни на физическите лица и на трети лица съобразно Регламент (ЕС) 2016/679 на ЕС и ЗЗЛД.

ГЛАВА ВТОРА

II. ЦЕЛИ И ОБХВАТ НА ПРАВИЛАТА

Чл. 2. Настоящите Правила имат за цел да регламентират:
(1) механизмите за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни;
(2) задълженията на Администратора, лицата обработващи лични данни, длъжностното лице по защита на лични данни и тяхната отговорност при неизпълнение на тези задължения;
(3) правилата за разпределение на личните данни и групирането им в регистри и Правилата за работа с личните данни;
(4) необходимите технически и организационни мерки за защита личните данни от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).
Чл. 3. Тези вътрешни правила се прилагат за личните данни по смисъла на Закона за защита на личните данни и са задължителни за всички лица имащи достъп до личните данни, обработвани за нуждите на администратора.

ГЛАВА ТРЕТА

III. ПРЕДНАЗНАЧЕНИЕ И ВИДОВЕ РЕГИСТРИ

Чл. 4. (1) В изпълнение на дейностите си Институцията поддържа регистри на лични данни.
1. Вътрешноведомствени регистри, които съдържат информация и се поддържат с цел обслужване дейностите по управление на персонала, счетоводната отчетност и деловодното обслужване:
1.1. Регистър „Счетоводство“
1.2. Регистър „Човешки ресурси“
1.3. Регистър „Трудови договори“
1.4. Регистър „Издадени УП”
1.5. Регистър „Дарения”
1.6. Регистър „Документи на неназначени служители”

2. Оперативни регистри, в които се набира, съхранява и обработва информация, необходима за целите на изпълнение на законови задължения на администратора:
2.1. Регистър на „Трудови злополуки“
2.2. Регистър на „Издадените дипломи за средно образование”
2.3. Регистър на „Издадените свидетелства за основно образование”
2.4. Регистър на „Издадените удостоверения за завършен клас”
2.5. Регистър на „Издадените дубликати на удостоверения за завършен клас”
2.6. Регистър на „Издадените удостоверения за завършена степен на образование”
2.7. Регистър на „Издадените дубликати за завършена степен на образование”
2.8. Регистър на „Издадените дубликати на документи за завършено образование”

3. Регистри, който обслужват задължения за регистрация/вписване на информация:
3.1. Регистър „Приети ученици”
3.2. Регистър „Неприети ученици”

Регистрите набират и съхраняват лични данни на СУ „Христо Ботев” с оглед:
1. Изпълняване целите на образователно-възпитателния процес;
2. Спазване на трудовото законодателство;
3. Спазване на Закона за счетоводството;

(2) Подробно описание на регистрите включително категории физически лица, за които се обработват лични данни, групи обработвани данни, източници и средства за събирането им, форма за водене на регистъра, ред за съхраняване и унищожаване на информационни носители, служители, обработващи лични данни, техническите ресурси, прилагани за обработване на данните в електронните регистри и други се съдържа в Приложенията, неразделна част от настоящите Вътрешни правила.
(3) Вътрешните правила се приемат с цел да регламентират:
1. Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;
2. Видовете регистри, които се водят в СУ „Христо Ботев” – Габарее: „Персонал”, „Обучавани”, „Контрагенти” и „Дневници”, както и тяхното описание.
3. Необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно

унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).
4. Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.
(4) Създаването на нови регистри и извършването на промени се извършва със заповед на Директора на Администратора.

ФОРМИ НА ВОДЕНЕ НА РЕГИСТЪРА
Чл. 5. (1) Формите на водене на регистрите биват на хартиен и технически носител.
1.Водене на регистър на хартиен носител:
1.1. Форма на организация и съхраняване на личните данни – писмена (документална); в електронен вариант
1.2.Местонахождение:
1.2.1. За учениците – Дирекция;
1.2.2. За персонала – в кабинет на ЗАС.
(2) Носител (форма) за предоставяне на данните от физическите лица – хартиен носител. Личните данни от лицата се подават на администратора на лични данни и оправомощеното лице, назначено за обработването им – обработващ лични данни, на основание нормативно задължение във всички случаи, когато е необходимо;
1. Достъп до личните данни – такъв има само обработващият лични данни.
(3) Водене на регистър на технически носител:
1. Форма на организация и съхраняване на личните данни – личните данни се съхраняват на твърд диск, на компютър;
2. Местонахождение на компютъра:
1.2.1. За учениците – в дирекцията;
1.2.2. За персонала – в дирекцията и в кабинет на ЗАС.
3. Достъп до личните данни и защита - достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият лични данни чрез парола за отваряне на тези файлове, както и длъжностното лице по защита на личните данни посредством делегирани му права и задължения от администратора на лични данни.

ГРУПИ ДАННИ В РЕГИСТЪРА
Чл. 6. (1) В зависимост от нормативното основание за събирането и предназначението им в регистрите се набират, обработва и съхраняват лични данни относно:
1. физическата идентичност на лицата – имена, ЕГН, номер на документ за самоличност, дата и място на издаването му, адрес, месторождение, телефони за контакт;
2. семейна идентичност на лицата – семейно положение, брой членове на семейството, родствени връзки и др.;
3. образование – вид на образованието, място, номер и дата на издаването на дипломата, допълнителна квалификация и др.;
4. трудова дейност – професионална биография, дни в осигуряване, осигурителен доход, основание за осигуряване, осигурени социални рискове, трудови договори, осигурители и други;
5. медицински данни – здравен статус, медицински диагнози и заключения на медицинската експертиза на временната и трайна неработоспособност;

6. други лични данни – осигурителен доход, трудови възнаграждения, парични обезщетения, статус на лицето (осъждано/неосъждано/реабилитирано) и други.
(2) Личните данни в регистрите се събират от администратора на лични данни на хартиен или електронен носител.

ЗАДЪЛЖЕНИЯ НА ЛИЦЕТО, ОТГОВАРЯЩО ЗА ВОДЕНЕ И СЪХРАНЯВАНЕ НА ДАННИТЕ В РЕГИСТРИТЕ
Чл. 7. Задълженията на лицето, отговарящо за водене и съхраняване на данните в регистъра (оправомощеното лице) включват набиране, обработване, актуализация и съхраняване на лични данни.

ПЕРИОДИЧНО АРХИВИРАНЕ
Чл. 8. Архивиране на личните данни на технически носител се извършва периодично на всяка 1 година от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид.

КОНТРОЛ ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ
Чл. 9. Контролът върху дейностите по обработка на лични данни се осъществява от Директора на образователната институция - администратор на лични данни.

АКТУАЛИЗАЦИЯ НА ЛИЧНИ ДАННИ
Чл. 10. (1) Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в дружеството. Актуализация на лични данни се извършва:
1. по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях, и удостовери това с документ;
2. по инициатива на обработващия лични данни – при наличие на документ, даващ основание за актуализация;
3. при установена грешка при обработката на личните данни от страна на обработващия лични данни;
(2) При актуализация на лични данни в досието на съответното лице се отразяват регистрационния номер на документа, източник на данните за актуализацията, дата на актуализацията. Актуализацията се извършва от лицето, обработващо личните данни.

ГЛАВА ЧЕТВЪРТА

IV. ДОСТЪП ДО ЛИЧНИ ДАННИ
ОСИГУРЯВАНЕ НА ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ

Чл. 11. (1) Всяко физическо лице, както и служителите в СУ „Христо Ботев”, има право на достъп до отнасящите се до него лични данни, обработвани от администратора.
(2) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, администраторът предоставя на съответното физическо лице достъп само за частта от данните, отнасяща се него.
(3) При упражняване на правото си на достъп физическото лице има право по всяко време да поиска от администратора на лични данни:

1. потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;
2. съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник.

(4) При смърт на физическото лице право на достъп до личните му данни имат неговите наследници.

Чл. 12. (1) Правото на достъп се осъществява с писмена молба до администратора на лични данни.

(2) Молбата може да бъде отправена и по електронен път по реда на Закона за електронния документ и електронния подпис.

(3) Молбата по ал. 1 се отправя лично от физическото лице или от изрично упълномощено от него лице чрез нотариално заверено пълномощно.

Чл. 13. (1) Молбата по чл. 12 съдържа:

1. трите имена, ЕГН/ЛНЧ/, адрес за контакт и телефон на заявителя;
2. описание на искането;
4. предпочитана форма за предоставяне на достъп до личните данни;
5. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на молба от упълномощено лице към същото се прилага и нотариално заверено пълномощно.

(3) При приемане на молбата, техническо лице извършва регистрация на същата в деловодната система на администратора.

Чл. 14. (1) Физическото лице може да поиска копие на обработваните лични данни на предпочитан носител или предоставянето им по електронен път, освен в случаите, когато това е забранено от закон.

(2) Администраторът на лични данни е длъжен да се съобрази с предпочитаната от молителя форма на предоставяне на информацията по чл. 11, ал. 3.

(3) Администраторът на лични данни предоставя исканата информация във форма, различна от заявената, когато:

1. за исканата форма няма техническа възможност;
2. исканата форма е свързана с необосновано увеличаване на разходите по предоставянето.

Чл. 15. (1) Администраторът на лични данни или изрично оправомощено от него лице разглежда молбата по чл. 11 и се произнася в 14-дневен срок от неговото постъпване.

(2) Срокът по ал. 1 може да бъде удължен от администратора до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(3) С решението си администраторът предоставя пълна или частична информация на заявителя или мотивирано отказва предоставянето й.

Чл. 16. Право на достъп до данните в поддържаните от администратора регистри на лични данни имат служителите в СУ „Христо Ботев”; администратори на базите данни, служителите, на които е възложено приемането и обработването на лични данни върху хартиен и електронен носител (обработващите лични данни), както и служителите, за които служебните им функции налагат такъв достъп.

Чл. 17. Служителите в СУ „Христо Ботев”с оторизиран достъп до лични данни са длъжни да обработват същите законосъобразно и добросъвестно, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели, както и да ги

поддържат във вид, който им позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които се обработват.

V. ДОСТЪП НА ТРЕТИ ЛИЦА ДО РЕГИСТРИТЕ СЪДЪРЖАЩИ ЛИЧНИ ДАННИ

Чл. 18. (1) Достъп до обработваните от администратора лични данни имат лицата, за които същия произтича от законово или договорно основание, както и органи по надзора или на съдебната власт (Комисия за финансов надзор, съд, прокуратура, следствени органи и др.). Достъпът на тези органи до личните данни на лицата е правомерен.
(2) Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на училището.
(3) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досиета на персонала.
(4) Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица в 30-дневен срок от подаване на молбата, респ. искането.

ГЛАВА ПЕТА
ВИДОВЕ ЗАЩИТА НА ЛИЧНИ ДАННИ
VI. ЛИЦАТА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 19. (1) За обезпечаване на адекватна защита на регистрите с лични данни администраторът може да определи лице/лица по защита на личните данни.
(2) Лицето/лицата по защита на личните данни има следните правомощия:
1. осигурява организация по водене на регистрите и мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;
3. осъществява контрол по спазване на изискванията по защита на регистрите;
4. специфицира техническите ресурси, прилагани за обработване на личните данни;
5. подпомага установяването на обстоятелства, свързани с нарушаване на защитата на регистрите;
6. в случай на установяване на нарушение на сигурността на личните данни, лицето по защита на личните данни уведомява в спешен порядък администратора на лични данни. Настъпилото събитие поражда задължение за администратора на лични данни в рамките на 72 часа от установяване на нарушението незабавно да уведоми КЗЛД за нарушаване сигурността на личните данни СУ „Христо Ботев”;
7. поддържа връзка с Комисията за защита на личните данни (КЗЛД) относно предприетите мерки и средства за защита на регистрите;
8. контролира спазването на правата на потребителите във връзка с регистрите и програмно техническите ресурси за тяхната обработка;

9. периодично информира персонала по въпросите на защитата на личните данни;
10. следи за спазване на организационните процедури за обработване на личните данни и провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Чл. 20. (1) С цел недопускането на неправомерен достъп, както и всички други незаконни форми на обработване на личните данни, администраторът организира и предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

(2) Видове защита:

1. Физическа защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.
2. Персонална защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.
3. Документална защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.
4. Защита на автоматизираните информационни системи и/или мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.
5. Псевдонимизация чрез употребата на технически и организационни мерки.

Чл. 21 (1) Всяко лице, желаещо да внесе документ съдържащ лични данни предоставя същия в деловодството на СУ „Христо Ботев” Лицето, приемащо документа е задължено да запознае вносителят на документите с правата му на субект на лични данни, както и с Вътрешните правила за тяхната обработка. Преди приемането му, вносителят попълва съответна Декларация по образец предоставена му от лицето, приемащо документите за деклариране на предоставените лични данни и основанието, на което те се предоставят и ще се ползват. Лицето, приемащо документите има право да изиска от субекта на лични данни документа, доказващ истинността на предоставените лични данни, а при наличие на предвидена в закона възможност, да снима копие от този документ и да го приложи към декларацията.

(2) Внесените документи с лични данни се докладват на Директора, който ги разпределя на лицата обработващи съответните лични данни.

(3) Лицата, обработващи личните данни са задължени да предоставят личните данни в съответствие с разпореждането на Директора на образователната институция - администратор на лични данни.

(4) Лични данни се предоставят на трети лица само чрез Директора на образователната институция - администратор на лични данни.

(5) При предоставяне на личните данни за ползване то трети лица, те попълват декларация за задължението си да обработват личните данни съгласно Регламент 2016/679 и ЗЗЛД.

VII. МЕРКИ ЗА ЗАЩИТА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 22. (1) Правилата за защита при обработване на лични данни регламентират технически мерки, които:

1. отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;

2. предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители – контрол на информационните носители;
3. предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни – контрол по съхраняването;
4. предотвратяват използването му от неоторизирани лица, използващи комуникационно оборудване за данни – контрол на потребителите;
5. гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп само до данните, включени в обхвата на техния достъп – контрол на достъпа до данни;
6. осигуряват възможността за проверка и установяване до кои органи са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудване за данни – контрол на комуникациите;
7. осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните – контрол на въвеждане;
8. предотвратяват неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;
9. осигуряване на възможност инсталираните системи да могат да се възстановят в случаи на прекъсване на функционирането – възстановяване;
10. осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата – интегритет.

Чл. 23. (1) Служителите, обработващи лични данни, вземат мерки за гарантиране на надеждност при обработването, като осъществява/т технически и организационни мерки за защита на личните данни.
(2) При автоматичната обработка на лични данни се осъществяват технически мерки за защита срещу:
1. неоторизирано четене, възпроизвеждане, промяна или премахване на носителя на данните;
2. неоторизирано въвеждане, промяна или заличаване на съхранени лични данни;
3.неоторизирано използване на системите за лични данни чрез средства за пренос на данни;
4.неоторизиран достъп до лични данни.

ГЛАВА ШЕСТА
VIII.ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Чл. 24. (1). Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.
(2) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.
Чл. 25. При оценката на въздействието администраторът отчита характера на обработваните лични данни, както следва:

1. систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение и др.
2. данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном;
3. лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;
4. лични данни в широкомащабни регистри на лични данни;
5. данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

IX. НИВА НА ВЪЗДЕЙСТВИЕ

Чл. 26. Определят се следните нива на въздействие:
1. „Изключително високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група
физически лица или трайни здравословни увреждания или смърт на група физически лица;
2. „Високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;
3. „Средно” – в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;
4. „Ниско” – в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл. 27. (1) Администраторът извършва оценка на въздействие за всички поддържани регистри .
(2) Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.
(3) Най-високото ниво на въздействие, определено по всеки от критериите по ал.2, определя нивото на въздействие на съответния регистър.

Чл. 28. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

Чл. 29. (1) Нивата на защита са ниско, средно, високо и изключително високо.
(2) Нивата на защита са, както следва:
1. при ниско ниво на въздействие – ниско ниво на защита;
2. при средно ниво на въздействие – средно ниво на защита;
3. при високо ниво на въздействие – високо ниво на защита;

4. при изключително високо ниво на въздействие – изключително високо ниво на защита.

ГЛАВА СЕДМА
X. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ И УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ

Чл. 30. (1) При възникване и установяване на инцидент и/или нерегламентиран достъп, свързан с нарушаване защитата или загуба на лични данни, незабавно се докладва на Директора на образователната институция - администратор на лични данни;
(2) За инцидентите се води регистър, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.
(3) След анализ от лицето по защита на личните данни, в регистъра се записват последствията от инцидента и мерките, които са предприети за отстраняването им.
(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни, като това се отразява в регистър по архивиране и възстановяване на данни.
(5) В случаите на компрометиране на парола, тя се подменя с нова, като събитието се отразява в регистъра за инциденти.

X. ОТГОВОРНОСТ

Чл. 31. За неизпълнение на задълженията, вменени на съответните оправомощени лица по тези Правила, по ЗЗЛД и по Регламент (ЕС) 2016/679, се налагат дисциплинарни наказания по българското законодателство, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – предвиденото в ЗЗЛД административно наказание, ако такава отговорност се предвижда по закон.
Чл. 32. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители в СУ „Христо Ботев”, засегнатите лица могат да търсят отговорност от виновните лица по реда на общото гражданско законодателство или наказателна отговорност, ако извършеното представлява престъпление.
(2) Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение, са причинени щети на администратора на лични данни на виновните лица се търси имуществена отговорност по Кодекса на труда или Закона за държавния служител.

Настоящите правила са утвърдени на ……14……..09.2020 година. за всички неуредени случаи се прилагат разпоредбите на Регламент 2016/679, ЗЗЛД и разпорежданията на Директора на образователната институция - администратор на лични данни.

Общо събрание 08.09.2020 г.

1. Приемане Правила за поведение при съмнение или случай на Ковид – 19
2. Етичен Кодекс
3. ПВТР
4. Правила за организиране и провеждане на образователен процес и за работа преа учебната 2020/2021 година в условията на Ковеид -19
5. Обсъждане - Правила за поведение при съмнение или случай на COVID-19 през учебната 2020/2021 година
6. ВП за предоставяне на административни услуги.
   / приема се на общо събрание/
7. ВП за мерките и средствата за образование и защита на личните данни **/ приема се на общо събрание/**