18. СРЕДНО УЧИЛИЩЕ "УИЛЯМ ГЛАДСТОН"

гр. София – 1303, ул. "Пиротска" № 68, тел. 02/988-03-01; e-mail: info-2204018@edu.mon.bg;

УТВЪРДИЛ:
РАЛИЦА КИРИЛО
ДИРЕКТОР НА
18 СУ „УИЛЯМ ГЛАДСТОН"

ПОЛИТИКА ЗА ИЗПЪЛНЕНИЕ НА ЗАДЪЛЖЕНИЯТА КАТО АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ ПО ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ И ДОКАЗВАНЕ НА ТОВА ИЗПЪЛНЕНИЕ НА 18 СРЕДНО УЧИЛИЩЕ „УИЛЯМ ГЛАДСТОН"

1 ОБЩИ ПОЛОЖЕНИЯ

Настоящите правила се приемат в изпълнение на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)/Регламента/ и Закона за защита на личните данни /ЗЗЛД/.

С настоящите правила се определят правилата, условията и реда за обработване на лични данни, приложими в дейността на **18 СУ „Уилям Гладстон"** в качеството му на администратор на лични данни по смисъла на Регламента.

1.1 Настоящите правила се приемат с цел да регламентират:

1. Създаването на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот и правото на защита на личните данни, чрез осигуряване на защита на физическите лица, при обработване на свързаните с тях лични данни, в процеса на свободно движение на данните.

2. Въвеждане на регистър на дейностите по обработване на данни (чл. 30 от Регламента).

3. Изпълнение на задълженията за прозрачност и информация, свързана с обработването на лични данни и упражняването на правата на субектите на данни (чл.12-14 от Регламента).

4. Извършване на оценка на риска (във връзка чл. 32 от Регламента).

5. Извършване на оценка на въздействието върху защитата на личните данни, ако е приложимо, по-специално, когато оценката на риска покаже висок риск (напр. в резултат на профилиране, мащабно обработване на специални (чувствителни) лични данни, систематично мащабно наблюдение на публично достъпна зона, нови технологии и др. съгласно списъка на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на личните данни, който следва да бъде приет от Комисията за защита на личните данни) (чл.35 от Регламента).

6. Определяне на подходящи технически и организационни мерки за осигуряване на сигурност на обработването (чл. 32 от Регламента)

7. Извършване на вътрешен анализ с оглед на вземането на решение дали да бъде определено ДЛЗД или не (във връзка с чл.37 от Регламента)

8. Осигуряване изпълнението на задължението за защита на данните на етапа на проектирането и по подразбиране (чл. 25 от Регламента)

9. Осигуряване на условия за изпълнение на задължението за уведомяване на КЗЛД и евентуално на субектите на данни при настъпване на нарушения на сигурността на данните (чл.33 и чл.34)

10. Осигуряване упражняването на правата на субектите на данни (глава 3 от Регламента)

11. Дефинирането на клаузи съгласно изискванията на чл. 28 от Регламента за включване на същите в договорите с обработващи лични данни във връзка с възлагането на обработване на лични данни.

1.2 Обработването и защитата на личните данни в 18 СУ „Уилям Гладстон“ става при спазване на принципите по чл. 5 от Регламента, както следва:

- ✓ Личните данни се обработват при наличие на правно основание – изпълнение на законови задължения, произтичащи от Закона за предучилищното и училищното образование и подзаконовите нормативни актове в областта на образованието, Закона за задълженията и договорите, Закона за обществените поръчки, Закона за счетоводството, Кодекса на труда, Кодекса за социално осигуряване, Закона за достъп до обществена информация, Закона за мерките срещу изпирането на пари и др.) или друго приложимо за случая правно основание. Категориите субекти на данни са уведомени за приложимите правни основания и се гарантира прозрачност за тяхната обработка („**законосъобразност, добросъвестност и прозрачност**“);
- ✓ Личните данни се събират само за конкретни, изрично указани и легитимни цели спазвайки принципа на **„ограничение на целите“** /конкретните цели са посочени в описанието за всеки регистър/;

✓ Личните данни, които се събират, са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („**свеждане на данните до минимум**“) /данните са посочени в описанието на всеки регистър/

✓ Данните за физическите лица се събират от самите физически лица, а в нормативно предвидени случаи – от други източници, поддържат се в актуално състояние и са точни, администраторът предприема всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват **(„точност);**

✓ Личните данни се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни („**ограничение на съхранението**“) /сроковете са посочени в описанието на всеки регистър/

✓ Личните данни се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки за сигурност при отчитане на рисковете за правата и свободите на ФЛ („цялостност и поверителност);

1.3 18 Средно училище „Уилям Гладстон“ носи отговорност и е в състояние да докаже спазването на принципите по т.1.2. („отчетност“), като води документация за отчетност, съгласно правилата на настоящата политика.

2 ВЪВЕЖДАНЕ НА РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ДАННИ (ЧЛ. 30 ОТ РЕГЛАМЕНТА)

2.1 Данни, които идентифицират администратора:

Администратор на лични данни е **18 Средно училище „Уилям Гладстон“, което, на основание чл. 25, ал. 1 от Закона за предучилищното и училищното образование,** е институция в системата на предучилищното и училищното образование, в която се обучават, възпитават и социализират ученици и се осигуряват условия за завършване на клас и етап и за придобиване на степен на образование. Училището е юридическо лице, регистрирано с БУЛСТАТ 000669190, със седалище и адрес на управление: гр. София, район Възраждане, п.к. 1303, ул. „Пиротска“ № 68. Данни за кореспонденция и контакт:

- адрес: гр. София, район Възраждане, п.к. 1303, ул. „Пиротска“ № 68
- Тел: 02/988 03 01;
- E-mail: info18@su.bg

2.2 В 18 СУ „Уилям Гладстон“ се обработват лични данни в следните регистри:

1. Регистър „Персонал“
2. Регистър „Ученици“
3. Регистър „Родители“
4. Регистър „Контрагенти“
5. Регистър „Лични лекари“
6. Регистър „Пропускателен режим“
7. Регистър „Достъп до обществена информация“
8. Регистър „ Видеонаблюдение“

3 РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

За всяка от дейностите по обработване се попълва следната информация:

- Основание за обработка;
- Целите на обработването
- Описание на категориите субекти на данни
- Описание на категориите лични данни;
- Източници от които се събират данните
- Категориите получатели, на които ще бъдат разкрити данните, в т.ч. и получателите в трети държави или международни организации;
- Събиране и начин на обработване;
- Предвидените срокове за изтриване на различните категории данни;
- Общо описание на техническите и организационни мерки за сигурност.

На тази база се създава Регистър на дейностите по обработване на лични данни.

4 ИЗПЪЛНЕНИЕ НА ЗАДЪЛЖЕНИЯТА ЗА ПРОЗРАЧНОСТ И ИНФОРМАЦИЯ, СВЪРЗАНА С ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ И УПРАЖНЯВАНЕТО НА ПРАВАТА НА СУБЕКТИТЕ НА ДАННИ (ЧЛ.12-14 ОТ РЕГЛАМЕНТА).

Служителите на 18 Средно училище „Уилям Гладстон“ се запознават с правилата в настоящата политика при назначаване. Информация за нея също така е включена и в програмата за обучение в областта на защитата на личните данни.

Физическите лица /Персонал, Ученици, Родители, Лични лекари, Посетители, Контрагенти/ предоставящи своите лични данни на 18 СУ се запознават с Политика за прозрачност при обработване на информацията посредством уебсайта на администратора www.18sou.net .

В допълнение, извлечение от политиката за прозрачност при обработване на информацията, насочена към ученици и родители, се предоставя на родителите/настойниците в момента на записване на техните деца в училището.

5 ИЗВЪРШВАНЕ НА ОЦЕНКА НА РИСКА (ВЪВ ВРЪЗКА ЧЛ. 32 И ЧЛ.35) НА ОСНОВАТА НА:

- ✓ естеството, обхвата, контекста и целите на обработването;
- ✓ възможните рискове за правата и свободите на физическите лица и тяхната вероятност и тежест;
- ✓ последиците за правата и свободите на физическите лица.

18 Средно училище „Уилям Гладстон“ е разработило следната Методология за оценка на риска.

Регистър за оценка на риска

6 ИЗВЪРШВАНЕ НА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ, КОГАТО ОЦЕНКАТА НА РИСКА ПОКАЖЕ ВИСОК РИСК (НАПР. В РЕЗУЛТАТ НА ПРОФИЛИРАНЕ, МАЩАБНО ОБРАБОТВАНЕ НА СПЕЦИАЛНИ (ЧУВСТВИТЕЛНИ) ЛИЧНИ ДАННИ, СИСТЕМАТИЧНО МАЩАБНО НАБЛЮДЕНИЕ НА ПУБЛИЧНО ДОСТЪПНА ЗОНА, НОВИ ТЕХНОЛОГИИ И ДР. СЪГЛАСНО СПИСЪКА НА ВИДОВЕТЕ ОПЕРАЦИИ ПО ОБРАБОТВАНЕ, ЗА КОИТО СЕ ИЗИСКВА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ, КОЙТО СЛЕДВА ДА БЪДЕ ПРИЕТ ОТ КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ) (ЧЛ.35 ОТ РЕГЛАМЕНТА).

Документирана процедура за анализ на необходимостта от оценка на въздействието:

С член 35 от Регламента /ОРЗД/ се въвежда понятието за оценка на въздействието върху защитата на данните (ОВЗД).

ОВЗД се изисква само когато съществува вероятност обработването *„да породи висок риск за правата и свободите на физическите лица*“ (член 35, параграф 1от Регламента).

За да се прецени дали съществува висок риск, за всяка от дейностите по обработване се извършва преценка дали попада в някои от следните хипотези:

- ✓ Събира ли се, използва ли се, съхранява ли се или споделят ли се чувствителни лични данни за граждани на ЕС?
- ✓ Извършва ли се систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице/„по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили“.

✓ Извършва ли се мащабно обработване на специални категории данни, посочени в член 9, параграф 1 или на лични данни за присъди и нарушения по член 10 /когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност/

✓ Извършва ли се систематично мащабно наблюдение на публично достъпна зона /всяко място, достъпно за гражданите, например площад, търговски център, улица, пазар, железопътна гара или обществена библиотека/

✓ Извършва ли се операции по обработване които възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор /Това включва операции по обработване, чиято цел е да се позволи, измени или откаже достъпът на субектите на данни до услуга или сключването на договор.

✓ Иновативно използват ли се или прилагат ли се нови технологични или организационни решения/ като например съчетаване на използването на пръстови отпечатъци и разпознаване на лица с цел подобряване на контрола на физическия достъп и др./

✓ Данни относно уязвими субекти на данни/Уязвимите субекти на данни могат да включват деца (може да се счита, че те не са в състояние съзнателно и мотивирано да възразят срещу или да се съгласят с обработването на техните данни), служители, по-уязвими сегменти от населението, които се нуждаят от специална защита (психично болни лица, търсещи убежище лица или възрастни лица, пациенти и др.) и субекти на данни във всички случаи, при които може да се установи неравнопоставеност в отношенията с оглед на положението на субекта на данни и това на администратора/

✓ Извършват ли се операции включени в "Списък на операциите по обработване на лични данни, за които ще се изисква извършване на оценка на въздействие съгласно чл. 35, § 4 от Общия регламент за защита на данните"/определени от КЗЛД/.

На база дейностите за обработка и горе посочените критерии е създаден Регистър за оценка на въздействието върху защитата на личните данни.

ОВЗД ще се извършва когато обработването отговаря на поне два от горепосочените въпроси или дейността по обработване попада в списъка на операциите на лични данни,за които ще се изисква извършване на оценка на въздействие.

Анализът показва, че не е необходимо да се извършва ОВЗД. В случай на промяна на някои от критериите, която би довела до необходимост от извършване на оценка на въздействието, администраторът ще извърши такава, при спазване на

изискванията за извършване на оценка на въздействието, ако законодателството е въвело такива. При липса на нормативно установени критерии за извършване на оценката на въздействието, при необходимост администраторът ще разработи собствена методология.

7 ОПРЕДЕЛЯНЕ НА ПОДХОДЯЩИ ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ОСИГУРЯВАНЕ НА СИГУРНОСТ НА ОБРАБОТВАНЕТО (ЧЛ. 32 ОТ РЕГЛАМЕНТА)

18 Средно училище „Уилям Гладстон“ с цел постигане на адекватно ниво на защита, прилага следните видове защита:

- **Физическа защита на личните данни, съдържащи се в Регистрите с лични данни**

1. Организационни мерки:

1.1. Определяне на зони с контролиран достъп; Всички физически зони с хартиени и електронни записи, се съхраняват и са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на работните им задължения. Всички записи и документи на хартиен носител, съдържащи лични данни са в заключени шкафове, които се намират в кабинети с ограничен достъп само за упълномощен персонал. Личните данни се обработват в съответствие с гореизложеното, според необходимостта да се знаят, в Човешките ресурси, в Счетоводството, в кабинетите на ресорните заместник-директори, на секретаря и в помещението на служебния архив.

1.2. Данните са защитени чрез използването на средства за физически контрол на достъпа, като заключване на вратите. Всички помещения, където се съхраняват данни на хартиен носител, се намират в зони с ограничен достъп - Счетоводството, Човешки ресурси, кабинетите на заместник-директорите, секретаря и служебния архив и са защитени чрез заключване на вратите, заключване на контейнерите или други подобни средства. Електронни носители, включително сървърът са защитени по подобен начин, в зони с контрол на климата /само за сървъра/.

1.3. Определяне на помещенията, в които ще се обработват лични данни. Личните данни се обработват в непублична част от помещенията, която е физически ограничена и достъпна само за служители, за които е необходимо да имат достъп с оглед на изпълнението на служебните им задачи. Личните данни на служителите се обработват от отдел Човешки ресурси, достъпът до който е ограничен само до оторизираните лица; личните данни на учениците и техните родители и лични лекари се обработват, според необходимостта, в кабинетите на ресорните заместник-директори, на секретаря и на служебния архив; личните данни, съдържащи се във финансови и счетоводни документи, се обработват в Счетоводството и в кабинета на заместник-директор „Административно-стопанска дейност“.

1.4. Определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни; Комуникационно-информационните системи, използвани за обработка на лични данни, са отделени от зоните

достъпни за посетители и са физически защитени, като достъпът е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните.

1.5. Определяне на организацията на физическия достъп;

Физически достъп до зоните с ограничен достъп, включително и тези, в които са намират информационните системи (компютри, сървър), е възможен само чрез заключени врати за достъп. Достъп се предоставя само на служителите, на които е пряко възложено това или от Счетоводство, на които той е необходим, за изпълнение на служебните им задължения, след оторизация.

1.6. Определяне на техническите средства за физическа защита.

2. Технически мерки

2.1. Ключалки

2.2. Шкафове

Шкафове с ограничен достъп се намират в отдел Счетоводство и Човешки ресурси, кабинет на заместник директор по АСД, с цел защита на регистрите с лични данни.

2.3. Оборудване на помещения.

2.4. Пожарогасителни средства.

- **Персонална защита**

1. Познаване на нормативната уредба в областта на защитата на лични данни – разглежда се в обучителната програма, която трябва да бъде премината от учителите и служителите и организирана от Училището. Същите са длъжни да прочетат и да се запознаят с правилата при наемането им, както и да преминават обучение, ако са налице промени в правилата на политиката.

2. Споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.) се забранява и се разглежда в обучителната програма, която трябва да бъде премината от служителите при наемането им и ако са налице промени в правилата на политиката.

3. Обучение

Служителите трябва да преминат обучение непосредствено след наемането им и ако са налице промени в правилата на политиката .

4. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

Тази тренировка се предоставя в обучението, което трябва да бъде преминато от служителите, непосредствено след наемането им и ако са налице съществени промени в правилата на политиката. Служителите следва незабавно да уведомят прекия си ръководител , ако имат съмнение или е известна заплаха за сигурността.

- **Документална защита**

1. Определяне на регистрите, които ще се поддържат на хартиен носител;

2. Определяне на условията за обработване на лични данни:

Личните данни се събират само с конкретна цел, за да подкрепят законните интереси на администратора на лични данни или доколкото е необходимо да се съобразят със законовите задължения на администратора на лични данни. Всеки тип данни се класифицира в съответствие с неговото предназначение и характер и са защитени в съответствие с изискванията, посочени по-горе.

3. Регламентиране на достъпа до регистрите:

Достъпът до регистрите е ограничен и се предоставя само на упълномощения персонал - училищното ръководство, човешки ресурси, счетоводство, секретар/деловодител и педагогически специалисти и непедагогически персонал, в съответствие с принципа на „Необходимост да знае".

4. Контрол на достъпа до регистрите:

Достъпът до данните ще бъде ограничен само до конкретни, минимално необходими данни, нужни на служителите, които имат необходимост да ги знаят за изпълнение на техните задължения.

5. Определяне на срокове за съхранение на личните данни

Съхраняването на данни е в съответствие с целите, за които са събрани данни и законоустановения срок. Личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани или както се изисква от приложимото право. Например ведомостите за заплати се съхраняват за 50 години след приключване на правоотношението, болничните листове – за срок от 3 години, считано от 1 януари на годината, следваща издаването им (чл. 56 от Наредбата за медицинската експертиза). След изтичането на определения срок или при отпаднало основание, данните трябва да бъдат изтрити/унищожени по безопасен начин.

6. Правила за размножаване и разпространение на лични данни

Личните данни могат да бъдат размножавани само ако това е в съответствие с целите на тяхното обработване, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа при спазване на принципа „необходимост да се знае".

7. Процедури за унищожаване

Документи на хартиен носител, които съдържат лични данни, трябва да бъдат унищожени по сигурен начин, когато вече не са необходими за училищни дейности или изпълнение на законови задължения за съхранение, чрез шредиране или чрез изгаряне. Проекти на документи, работни копия и др. подобни, съдържащи лични данни се унищожават незабавно след приключване на работатата с тях от съответния служител

Защита на автоматизираните информационни системи и/или мрежи

1. Идентификация и автентификация

1.1.Потребителски акаунти и пароли - с цел да се въведе достъп, съобразен с принципа "Необходимост да знае", Училището изисква мултипотребителските информационни системи да прилагат уникални потребителски акаунти и лични пароли за всеки потребител с акаунт за достъп до мрежата.
1.2. Отговорност на целия персонал - членовете на персонала са лично отговорни за правилното използване на техните потребителски акаунти и пароли.

2. Управление на регистрите – длъжностите, които имат достъп до личните данни в отделните регистри с лични данни, се определят със заповед на директора на 18 СУ „Уилям Гладстон“. Заповедта е неразделна част от настоящата политика.

3. Телекомуникации и достъп
Интернет достъп - на членовете на персонала може да бъде предоставен достъп до интернет, за да изпълняват служебните си задължения, но индивидуалният достъп може да бъде прекратен по всяко време по преценка на Училището. Цялата информация, получена чрез интернет, трябва да бъде под съмнение, докато не бъде потвърдена от надеждни източници. Членовете на екипа не трябва да предоставят информация относно Училището, независимо дали съдържа или не лични данни, на каквато и да е публично достъпна компютърна система, като Интернет, освен ако това е било одобрено от Директора или оторизираното лице, отговорно за личните данни за съответния регистър.

4. Защита от вируси
4.1. Училището създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира. Системният софтуер се контролира и се поддържа от оторизирани лица.
Антивирусният софтуер скрининг трябва да се използва, за да сканира всички софтуери и файлове с данни, идващи от или до трети страни или други групи на Училището. Членовете на екипа не трябва да избягват или да изключват сканиране на процесите, които биха могли да предотвратят предаването на компютърни вируси. Дискове и други магнитни носители, използвани от заразен компютър не трябва да се използват на друг компютър, докато вирусът не бъде успешно премахнат. Заразеният компютър също трябва да бъде незабавно изолиран от вътрешните мрежи, ако се изградят такива.

4.2. Поддържане/експлоатация

Оценка на сигурността и тестване – Училището периодично ще провежда оценки на сигурността, уязвимостта и тестове за проникване в системи и мрежи /в случай, че бъдат изградени такива/. Училището ще провежда оценки за сигурността на информацията и/или неприкосновеността на личните данни, членовете на персонала не трябва да придобиват, притежават, търгуват или използват хардуерни или софтуерни инструменти, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Примери за такива инструменти са тези, които поразяват софтуера за защита на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Без одобрение на прекия ръководител или по-горестоящ, е забранено използването на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа /в случай, че се изгради такава/ или опериращ компютър. Неоторизирано използване на такива инструменти може да доведе до дисциплинарни действия.

4.3. Копия/резервни копия за възстановяване

Архивиране на информацията - Целта на Училището е да поддържа наличността на информацията. Информацията, съдържаща лични данни трябва да бъде архивирана в съответствие със стандартите за архивиране на данни. Ако бъде необходимо, трябва да се инсталира или предостави техническа помощ за инсталирането на резервен хардуер. Всички архиви, съдържащи данни за поверителна и / или училищна информация, трябва да се съхраняват с физически контрол на достъпа.

4.4. Физическа среда/обкръжение

Физически контрол включително заключени врати, поддържане на подходяща температура и нива на влажност и наличието на детектори за пожар и пожарогасителната система са осигурени за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

4.5. Персонална защита

4.6. Процедури за унищожаване/заличаване/изтриване на носители:

Данни, които вече не са необходими за целите, за които се обработват или при наличие на друго основание по чл. 17, пар. 1 от Регламента, трябва да бъдат изтрити/унищожени чрез средства, които не позволяват изцяло или частично възстановяване на информацията, като шредиране, изгаряне или необратимо заличаване от електронните средства.

План при извънредни ситуации – действията на училищното ръководство и персонал при извънредни ситуации се осъществяват в съответствие със Закона за защита при бедствия и в рамките на училищния План за защита при бедствия.

Директорът на училището е отговорен за контрола по управлението на регистрите.

Само оправомощени лицата имат достъп до регистъра.

За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа за цялата сграда, сигнално-охранителна система.

След постигане целта на обработване на личните данни или преди преустановяване на обработването на личните данни в регистрите администраторът е длъжен да ги унищожи съгласно „Процедура за унищожаване на документите съдържащи лични данни при **18 Средно училище „Уилям Гладстон“** (Приложение № 12) и при спазване на общите правила за архивната дейност в училищата.

8 ИЗВЪРШВАНЕ НА ВЪТРЕШЕН АНАЛИЗ С ОГЛЕД НА ВЗЕМАНЕТО НА РЕШЕНИЕ ДАЛИ ДА БЪДЕ ОПРЕДЕЛЕНО ДЛЗД ИЛИ НЕ(ВЪВ ВРЪЗКА С ЧЛ. 37 ОТ РЕГЛАМЕНТА);

18 Средно Училище „Уилям Гладстон“ е публична структура по смисъла на чл. 37, пар.1, б. „а“ от Общия регламент, поради което е задължено да определи Длъжностно лице по защита на данните.

9 ОСИГУРЯВАНЕ ИЗПЪЛНЕНИЕТО НА ЗАДЪЛЖЕНИЕТО ЗА ЗАЩИТА НА ДАННИТЕ НА ЕТАПА НА ПРОЕКТИРАНЕТО И ПО ПОДРАЗБИРАНЕ, КОГАТО Е ПРИЛОЖИМО (ЧЛ. 25 ОТ РЕГЛАМЕНТА);

9.1 Защита на личните данни на етапа на проектирането

18 Средно училище „Уилям Гладстон“ предприема подходящи технически и организационни мерки преди започването на обработката на лични данни (на етапа определяне на целите и средствата за обработване), като осигурят тяхното прилагане през целия жизнен цикъл на данните.

Такива подходящи мерки са псевдонимизация и/или криптиране на данните, залагане на функционалности за автоматизирано отчитане на сроковете за съхранение и автоматичното им изтриване след изтичането им, минимизиране на видовете данни, които се събират, своевременно актуализиране на данните, както и съхраняване на доказателства за предприетите действия (логове) и др.

9.2 Защита на личните данни по подразбиране.

18 Средно Училище „Уилям Гладстон“ прилага механизми, които по подразбиране гарантират изпълнението на следните изисквания:

✓ Само минималното количество лични данни и операции по обработване, които са абсолютно необходими за постигането на всяка специфична цел, биват обработвани;

✓ Данните са съхранявани за минималния срок, абсолютно необходим за постигане на целите на обработване (съгласно приложимите законови и подзаконови нормативни актове) и след това заличени при спазване на съответните правила и процедури;

✓ Всеки достъп, предаване или споделяне на данни е допустим, само при наличие на валидно правно основание за това (например, съгласието на субекта на данни или правни задължения на администратора);

✓ Данните не стават достъпни до неограничен кръг от лица.

10 ИЗПЪЛНЕНИЕ НА ЗАДЪЛЖЕНИЕТО ЗА УВЕДОМЯВАНЕ НА КЗЛД И ЕВЕНТУАЛНО НА СУБЕКТИТЕ НА ДАННИ ПРИ НАСТЪПВАНЕ НА НАРУШЕНИЯ НА СИГУРНОСТТА (ЧЛ.33 И ЧЛ.34);

10.1.1 Уведомление на КЗЛД за нарушение на сигурността на личните данни

При възникване и установяване на нарушение на сигурността на личните данни, веднага се докладва на Директора на училището. За нарушенията се води дневник Приложение – дневник на нарушенията, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на нарушението, упълномощено лице вписва в дневника последствията от нарушението и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Директора на училището, като това се отразява в дневника.

18 СУ „Уилям Гладстон“ без ненужно забавяне и когато това е осъществимо — **не по-късно от 72 часа** след като е разбрал за него, уведомява за нарушението на сигурността на личните данни КЗЛД, освен когато не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

Обработващият лични данни уведомява **18 СУ „Уилям Гладстон“** без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

В уведомлението се съдържа най-малко следното:

✓ описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

✓ посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

✓ описание на евентуалните последици от нарушението на сигурността на личните данни;

✓ описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

Когато и доколкото не е възможно информацията да се подаде едновременно, тя може да се подаде поетапно без по-нататъшно ненужно забавяне.

Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на надзорния орган да провери дали е спазен закона.

10.2 Съобщаване на субекта на данните за нарушение на сигурността на личните данни

10.2.1 Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

10.2.2 Съобщение не се изисква, ако някое от следните условия е изпълнено:

✓ администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

✓ след настъпване на нарушението администраторът е взел мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

✓ то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

11 ОСИГУРЯВАНЕ УПРАЖНЯВАНЕТО НА ПРАВАТА НА СУБЕКТИТЕ НА ДАННИ (ГЛАВА 3 ОТ РЕГЛАМЕНТА):

Субектите на данни на **18 СУ „Уилям Гладстон“** имат право на :

✓ Информация относно личните си данни, които училището обработва ;

✓ Достъп до собствените си лични данни;

✓ Коригиране на личните данни (ако данните са неточни или непълни);

✓ Изтриване на личните данни;

✓ Ограничаване на обработването от страна на администратора или обработващия лични данни ;

✓ Право да получат данните си в структуриран, широко използван и пригоден за машинно четене формат и право да ги прехвърлят на друг администратор (право на преносимост)

✓ Възражение спрямо обработването на техни лични данни;

✓ Право и да не бъдат обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за тях или по подобен начин ги засяга в значителна степен;

✓ Право на защита по съдебен или административен ред, в случай че правата на субекта на данни са били нарушени. Всеки субект на данни, може да подаде жалба до Комисията за защита на личните данни или до съответния Административен съд по общите правила за подсъдност.

Надзорен орган в Република България е:

Комисия за защита на личните данни, Адрес: гр. София 1592, бул. „Проф. Цветан Лазаров" № 2, Уебсайт: https://www.cpdp.bg/

Лицата, които желаят да упражнят горепосочените си права подават писмено искане до **18 Средно училище „Уилям Гладстон"** или чрез упълномощено лице на определеното за ДЗЛД лице за кореспонденция и контакт, или по електронен път на следния имейл sou18@mail.net при условията на Закона за електронния документ и електронните удостоверителни услуги.

18 Средно училище „Уилям Гладстон" предлага следните бланки за упражняване на правата на субектите на данни:

✓ Приложение 6 – искане за достъп до личните данни;

✓ Приложение 7 – искане за коригиране на личните данни;

✓ Приложение 8 – искане за изтриване на личните данни;

✓ Приложение 9 – искане за ограничаване на обработването на личните данни;

✓ Приложение 10 – искане за преносимост на личните данни;

✓ Приложение 11 – искане за възражение спрямо обработването на личните данни.

Администраторът предоставя на субекта на данни информация относно действията, предприети във връзка с искането, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от

получаване на искането, като посочва и причините за забавянето. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.

Ако администраторът не предприеме действия по искането на субекта на данни, администраторът уведомява субекта на данни без забавяне и най-късно в срок от един месец от получаване на искането за причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган и търсене на защита по съдебен ред.

Информацията по исканията се предоставя безплатно. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може или:

а) да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия, или

б) да откаже да предприеме действия по искането.

Когато администраторът има основателни опасения във връзка със самоличността на физическото лице, което подава искането, администраторът може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.

12 ДОКУМЕНТИРАНИ КЛАУЗИ СЪГЛАСНО ИЗИСКВАНИЯТА НА ЧЛ. 28 ОТ РЕГЛАМЕНТА ЗА ВКЛЮЧВАНЕ НА СЪЩИТЕ В ДОГОВОРИТЕ С ОБРАБОТВАЩИ ЛИЧНИ ДАННИ ВЪВ ВРЪЗКА С ВЪЗЛАГАНЕТО НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ.

С цел привеждане на дейността на обработващия в съответствие с чл. 28 от Регламента, администраторът ще предприеме действия по изменения и допълнения на сключените договори с включване на **„ Клаузи за защита на личните данни между Администратор и Обработващ лични данни”.**

Администраторът може да приеме и клаузи с подобно съдържание, покриващо изискванията на чл. 28 от Регламента, предоставени с договора от доставчиците на услуги.

Политиката е задължителна за всички служители на 18 СУ „Уилям Гладстон“ и те са длъжни да се запознаят срещу подпис и да я спазват.

Контрол по изпълнението на настоящата политика се осъществява от Директора на **18 Средно училище „Уилям Гладстон“**.

Изменения и допълнения на тази политика се правят по реда на издаването и утвърждаването ѝ.

Тази политика е утвърдена със заповед № 2641/25.05.2018 г. и е в сила от 25.05.2018 г., изменена и допълнена съгласно Заповед № 2891/05.09.2019 г. и Заповед № 1781/31.08.2020 г. и заповед № РД-17-3074/18.08.2025 г.

Приета на 31.06.2025 г. с протокол № 80 от 31.06.2025 г. на Общо събрание и утвърдена заповед № РД-17-3074/18.08.2025 г.