



პერსონალურ მონაცემთა დამუშავების პოლიტიკა

მუხლი 1. პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტის არსი და მიზანი

პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტით აღწერილია შპს თაობა (შემდგომში - სკოლა) მიერ პერსონალური მონაცემების დამუშავების პროცესი და დამუშავების პროცესში მონაცემთა სუბიექტის უფლებათა დაცვის გარანტიები. პოლიტიკის მიზანია განსაზღვროს სკოლის მიერ, მისი მიზნებისა და საქმიანობის გათვალისწინებით, შეგროვებული პერსონალური მონაცემების დაცვისა და დამუშავების წესები და პროცედურები, უზრუნველყოს დამუშავების პროცესის კანონმდებლობის შესაბამისად წარმართვა, დაიცვას ფიზიკური პირის უფლებები და უზრუნველყოს დამუშავების გამჭვირვალობა.

ჩვენ ვაღიარებთ და განსაკუთრებულ მნიშვნელობას ვანიჭებთ მონაცემთა დაცვას, შესაბამისად, პერსონალურ მონაცემთა დამუშავებისას, ვმოქმედებთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის, სხვა ნორმატიული აქტებისა და პერსონალურ მონაცემთა დაცვის პოლიტიკის შესაბამისად და მივმართავთ უსაფრთხოებისთვის საჭირო ყველა ორგანიზაციულ და ტექნიკურ ზომას.

მუხლი 2. ინფორმაცია პერსონალურ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის შესახებ

თაობა - საქართველოს კანონმდებლობის შესაბამისად რეგისტრირებული, როგორც შეზღუდული პასუხისმგებლობის საზოგადოება

საიდენტიფიკაციო კოდი: 445474415

მისამართი: ქ. ბათუმი, რურუას ქ. N 10

ტელეფონის ნომერი: +995 597 020 706

ელექტრონული ფოსტა: schooltaoba@gmail.com

მუხლი 3. ინფორმაცია პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ

შპს „პრემიუმ სეიფთი“

საიდენტიფიკაციო კოდი: 405656320

მისამართი: ქ. თბილისი, ვაკის რაიონი, ყიფშიძის ქ N2, კორპუსი 2ბ, 73

ტელეფონის ნომერი: (+995) 557 692 449



მუხლი 4. ტერმინთა განმარტება

1. ამ წესში გამოყენებულ ტერმინებს ამავე წესის მიზნებისთვის აქვთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მნიშვნელობა:

ა) **პერსონალური მონაცემი (შემდგომ – მონაცემი)** – ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. ფიზიკური პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, მათ შორის, სახელით, გვარით, საიდენტიფიკაციო ნომრით, გეოლოკაციის მონაცემებით, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემებით, ფიზიკური, ფიზიოლოგიური, ფსიქიკური, ფსიქოლოგიური, გენეტიკური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლით;

ბ) **განსაკუთრებული კატეგორიის მონაცემი** – მონაცემი, რომელიც უკავშირდება ფიზიკური პირის რასობრივ ან ეთნიკურ კუთვნილებას, პოლიტიკურ შეხედულებებს, რელიგიურ, ფილოსოფიურ ან სხვაგვარ მრწამსს, პროფესიული კავშირის წევრობას, ჯანმრთელობას, სქესობრივ ცხოვრებას, ბრალდებულის, მსჯავრდებულის, გამართლებულის ან დაზარალებულის სტატუსს სისხლის სამართლის პროცესში, მსჯავრდებას, ნასამართლობას, განრიდებას, ადამიანით ვაჭრობის (ტრეფიკინგის) ან „ქალთა მიმართ ძალადობის ან/და ოჯახში ძალადობის აღკვეთის, ძალადობის მსხვერპლთა დაცვისა და დახმარების შესახებ“ საქართველოს კანონის შესაბამისად დანაშაულის მსხვერპლად ცნობას, პატიმრობას და მის მიმართ სასჯელის აღსრულებას, აგრეთვე ბიომეტრიულ და გენეტიკურ მონაცემებს, რომლებიც ფიზიკური პირის უნიკალური იდენტიფიცირების მიზნით მუშავდება;

გ) **ჯანმრთელობასთან დაკავშირებული მონაცემი** – მონაცემთა სუბიექტის ფიზიკური ან ფსიქიკური ჯანმრთელობის შესახებ, აგრეთვე მისთვის სამედიცინო მომსახურების გაწევის თაობაზე ინფორმაცია, თუ იგი მონაცემთა სუბიექტის ფიზიკური ან ფსიქიკური ჯანმრთელობის შესახებ ინფორმაციას იძლევა;

დ) **ბიომეტრიული მონაცემი** – ტექნიკური საშუალებების გამოყენებით დამუშავებული, მონაცემთა სუბიექტის ფიზიკურ, ფიზიოლოგიურ ან ქცევის მახასიათებელთან (როგორიცაა, მაგალითად: სახის გამოსახულება, ხმის მახასიათებელი ან დაქტილოსკოპიური მონაცემები) დაკავშირებული მონაცემი, რომელიც მისი უნიკალური იდენტიფიცირების ან ვინაობის დადასტურების შესაძლებლობას იძლევა;

ვ) **მონაცემთა დამუშავება** – მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება, მათ შორის, მათი შეგროვება, მოპოვება, მათზე წვდომა, მათი ფოტოგადაღება, ვიდეომონიტორინგი ან/და აუდიომონიტორინგი, ორგანიზება, დაჯგუფება, ურთიერთდაკავშირება, შენახვა, შეცვლა, აღდგენა, გამოთხოვა, გამოყენება, დაბლოკვა, წაშლა ან განადგურება, აგრეთვე მონაცემთა გამჟღავნება მათი გადაცემით, გასაჯაროებით, გავრცელებით ან სხვაგვარად ხელმისაწვდომად გახდომით;

ზ) **მონაცემთა ავტომატური საშუალებებით დამუშავება** – მონაცემთა დამუშავება ინფორმაციული ტექნოლოგიების გამოყენებით;



თ) **მონაცემთა არაავტომატური საშუალებებით დამუშავება** – მონაცემთა დამუშავება ინფორმაციული ტექნოლოგიების გამოყენების გარეშე;

ი) **მონაცემთა ნახევრად ავტომატური საშუალებებით დამუშავება** – მონაცემთა დამუშავება ავტომატური საშუალებებისა და არაავტომატური საშუალებების ერთობლივი გამოყენებით;

კ) **ფაილური სისტემა** – მონაცემთა სტრუქტურიზებული წყება, რომელშიც ისინი დალაგებული და ხელმისაწვდომია კონკრეტული კრიტერიუმის მიხედვით;

ლ) **მონაცემთა სუბიექტი** – ნებისმიერი ფიზიკური პირი, რომლის შესახებ მონაცემიც მუშავდება;

მ) **მონაცემთა სუბიექტის თანხმობა** – მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე აქტიური მოქმედებით, წერილობით (მათ შორის, ელექტრონულად) ან ზეპირად, თავისუფლად და მკაფიოდ გამოხატული ნება;

ნ) **მონაცემთა სუბიექტის წერილობითი თანხმობა** – თანხმობა, რომელსაც მონაცემთა სუბიექტმა ხელი მოაწერა ან რომელიც მან სხვაგვარად გამოხატა წერილობით (მათ შორის, ელექტრონულად) მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე შესაბამისი ინფორმაციის მიღების შემდეგ;

ო) **დამუშავებისთვის პასუხისმგებელი პირი** – ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან დამუშავებაზე უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას;

პ) **თანადამუშავებისთვის პასუხისმგებელი პირები** – დამუშავებისთვის პასუხისმგებელი ორი ან ორზე მეტი პირი, რომლებიც ერთობლივად განსაზღვრავენ მონაცემთა დამუშავების მიზნებსა და საშუალებებს;

ჟ) **დამუშავებაზე უფლებამოსილი პირი** – ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც მონაცემებს ამუშავებს დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით. დამუშავებაზე უფლებამოსილ პირად არ მიიჩნევა დამუშავებისთვის პასუხისმგებელ პირთან შრომით ურთიერთობაში მყოფი ფიზიკური პირი;

რ) **მონაცემთა მიმღები** – ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელსაც მონაცემები გადაეცა, გარდა პერსონალურ მონაცემთა დაცვის სამსახურისა

ს) **ინციდენტი** – მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას.

2. ამ წესში მოცემული სხვა ტერმინები, სპეციალური მითითების არ არსებობის პირობებში, განიმარტება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად.



მუხლი 5. პერსონალურ მონაცემთა დამუშავებაზე უფლებამოსილი პირი

1. სკოლას ჰყავს მონაცემთა დამუშავებაზე უფლებამოსილი პირები, რომლებიც მონაცემებს ამუშავებენ მხოლოდ სკოლის ლეგიტიმური მიზნების განსახორციელებლად.
2. სკოლასა და უფლებამოსილ პირებს შორის გაფორმებულია შესაბამისი ხელშეკრულებები, რომლებიც, მათ შორის მოიცავს პერსონალურ მონაცემთა დაცვის საკითხების მოწესრიგებას და უფლებამოსილ პირ(ებ)ს ეკისრებათ მომსახურების ფარგლებში მათ მიერ დამუშავებული მონაცემების კონფიდენციალურობის უზრუნველყოფის ვალდებულება.
3. სკოლა ახორციელებს უფლებამოსილი პირების მიერ მათი ფუნქცია - მოვალეობების შესრულებისას ტექნიკურ - ორგანიზაციული ზომებისა და მონაცემების დამუშავების მონიტორინგს.
4. მოთხოვნის შემთხვევაში, სკოლა უზრუნველყოფს მონაცემთა სუბიექტ(ებ)ისთვის უფლებამოსილი პირ(ებ)ის შესახებ ინფორმაციის მიწოდებას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი წესით.

მუხლი 6. მონაცემთა სუბიექტები

სკოლა ამუშავებს შემდეგი ფიზიკური პირების პერსონალურ მონაცემებს:

- ა) მოქმედი და ყოფილი თანამშრომლები, მათ შორის, შრომითი ხელშეკრულებით დასაქმებული პირები;
- ბ) ვაკანტური პოზიციების დასაკავებლად გამოცხადებულ კონკურსში მონაწილე კანდიდატები;
- გ) მოსწავლეები;
- დ) მშობელი/კანონიერი წარმომადგენელი;
- დ) ვიდეთვალთვალის არეალში მოხვედრილი სხვა პირები.

მუხლი 7. მონაცემთა კატეგორია

მონაცემთა სუბიექტთან ურთიერთობის ხასიათიდან და მონაცემთა დამუშავების მიზნიდან გამომდინარე, საჭიროებისამებრ, შეიძლება დამუშავდეს შემდეგი პერსონალური მონაცემები:

მოქმედი და ყოფილი თანამშრომლები, მათ შორის, შრომითი ხელშეკრულებით დასაქმებული პირები -

- ა) პირადობის დამადასტურებელი დოკუმენტის ასლი;
- ბ) ფოტოსურათი ზომით 3X4;
- გ) ავტობიოგრაფია/CV;
- დ) განათლების დამადასტურებელი დოკუმენტის დედანი, ან ნოტარიულად დამოწმებული ასლი (მხოლოდ მასწავლებელზე);



ე) კვალიფიკაციის ამაღლების დამადასტურებელი დოკუმენტები, ასეთის არსებობის შემთხვევაში;

ვ) საგნის ჩაბარების დამადასტურებელი სერტიფიკატი/ცნობა, ასეთის არსებობის შემთხვევაში;

განსაკუთრებული კატეგორიის მონაცემები -

ზ) ცნობა ნასამართლეობის შესახებ;

თ) ცნობა სქესობრივი თავისუფლებისა და ხელშეუხებლობის წინააღმდეგ მიმართული დანაშაულის ჩადენისთვის ნასამართლეობის შესახებ;

ი) ნარკოლოგიური ცნობა;

კ) ჯანმრთელობის ცნობა.

ვაკანტური თანამდებობის დასაკავებლად გამოცხადებულ კონკურსში მონაწილე პირების მონაცემები -

ა) პირადობის დამადასტურებელი დოკუმენტის ასლი;

ბ) ფოტოსურათი ზომით 3X4;

გ) ავტობიოგრაფია/CV;

დ) განათლების დამადასტურებელი დოკუმენტის დედანი, ან ნოტარიულად დამოწმებული ასლი (მხოლოდ მასწავლებელზე);

ე) კვალიფიკაციის ამაღლების დამადასტურებელი დოკუმენტები, ასეთის არსებობის შემთხვევაში;

ვ) საგნის ჩაბარების დამადასტურებელი სერტიფიკატი/ცნობა, ასეთის არსებობის შემთხვევაში;

სკოლაში მოსწავლის ჩასარიცხად მშობელმა/კანონიერმა წარმომადგენელმა უნდა წარმოდგინოს შემდეგი საბუთები -

ა) განცხადება სკოლის დირექტორის სახელზე;

ბ) მოსწავლის ორი ფოტოსურათი (3X4);

გ) დაბადების მოწმობის ასლი;

დ) მშობლების პირადობის მოწმობების ასლები;

ე) ბავშვის ბინადრობის დამადასტურებელი დოკუმენტის ასლი (უცხო ქვეყნის მოქალაქის შემთხვევაში (ასეთის არსებობის შემთხვევაში));

ვ) მშობლის ბინადრობის დამადასტურებელი დოკუმენტის ასლი (უცხო ქვეყნის მოქალაქის შემთხვევაში(ასეთის არსებობის შემთხვევაში));

ზ) კანონიერი წარმომადგენლის უფლებამოსილების დამადასტურებელი დოკუმენტი (არსებობის შემთხვევაში);

თ) ჯანმრთელობის ცნობა.



მშობელზე/კანონიერ წარმომადგენელზე სკოლა, გარდა ზემოხსენებულისა, დამატებით ამუშავებს -

ა) ტელეფონის ნომრები;

ბ) იურიდიული ან/და ფაქტობრივი მისამართი.

ვიდეომონიტორინგის არეალში მოხვედრილი სხვა პირები.

მუხლი 8. მონაცემთა მიღების წყაროები

სკოლისთვის პერსონალურ მონაცემთა მიღების წყაროებია:

ა) მონაცემთა სუბიექტის აშკარა, აქტიურად გამოვლენილი თანხმობის (ასევე, რეკრუტინგის, გარიგების) საფუძველზე მონაცემების მიწოდება;

ბ) ზოგადი განათლების მართვის საინფორმაციო სისტემისა ან ელექტრონული ჟურნალის მონაცემთა ერთიანი ბაზიდან მონაცემების მიღება;

გ) სასწავლო პროცესის მიმდინარეობისას მონაცემთა შექმნა (პირადი საქმის, ელექტრონული ჟურნალის, დისტანციური სწავლების მოდულის და სხვა საშუალებებით);

დ) ვიდეომონიტორინგის განხორციელების გზით მოპოვებული მონაცემები;

ე) ამ წესით ან/და კანონით განსაზღვრული მიზნებით ნებისმიერი კანონიერი წყაროდან ინფორმაციის მოპოვება.¹

მუხლი 9. მონაცემთა დამუშავების მიზნები

სკოლის მიერ პერსონალურ მონაცემთა დამუშავების მიზნებია:

ა) ზოგადსაგანმანათლებლო საქმიანობის განხორციელება;

ბ) სასწავლო პროცესის, მათ შორის დისტანციური სწავლების შეუფერხებელი მიმდინარეობის უზრუნველყოფა;

გ) მოსწავლეთა რეგისტრაცია;

დ) მოსწავლეთა, თანამშრომელთა პირადი საქმეების წარმოება;

¹ სკოლამ ინფორმაცია შეიძლება მოიპოვოს:

1. საჯარო რეესტრებიდან, თუ ეს აუცილებელია სამართლებრივი ან ადმინისტრაციული მიზნებისთვის;
2. მესამე პირებისაგან, თუ ეს საჭიროა კონტრაქტის შესრულებისთვის ან მომსახურების მიწოდების უზრუნველსაყოფად ან საკუთარი ან მესამე პირების კანონიერი ინტერესების დასაცავად;
3. საჯარო ორგანიზაციებისა და ინსტიტუტებისგან, თუ ეს აუცილებელია საჯარო ინტერესის დაცვის მიზნით;
4. დასაქმების ონლაინ პლატფორმისგან, კერძოდ, <https://teacherjobs.ge/>;
5. <https://portal.emis.ge/my.policy> (eSchool);
6. <https://eservices.schoolbook.ge/>.



- ე) სპეციალური საგანმანათლებლო საჭიროების მქონე მოსწავლეთათვის განათლების უფლების რეალიზება;
- ვ) სკოლაში დასაქმების მსურველი კვალიფიციური კადრების რეკრუტირება;
- ზ) მოსწავლეთა აღრიცხვის, შეფასების, მათი მობილობის უზრუნველყოფა;
- თ) ელექტრონული ჟურნალების წარმოების მიზნით, მონაცემთა ბაზების სრულყოფა;
- ი) დოკუმენტრუნვის ორგანიზება და კონტროლი;
- კ) ზოგადი განათლების დამადასტურებელი დოკუმენტის გაცემა;
- ლ) სკოლის საკუთრების, ქონების დაცვის, თანამშრომელთა ან/და სტუმართა/მესამე პირთა ფიზიკური უსაფრთხოების უზრუნველყოფა;
- მ) სკოლის მხრიდან გაწეული მომსახურების ხარისხის გაუმჯობესება;
- ნ) ზემდგომი ორგანოებისთვის მოთხოვნილი ინფორმაციის მიწოდება;
- ო) მოსწავლეთა აკადემიური მიღწევის მაჩვენებლების შეგროვება;
- პ) მოსწავლეთა და დასაქმებულთა სხვადასხვა აქტივობებში ჩართვის უზრუნველყოფა;
- ჟ) სსიპ - განათლების მართვის საინფორმაციო სისტემისთვის მოთხოვნილი ინფორმაციის მიწოდება, მათ ბაზაში მონაცემების ატვირთვა;
- რ) კანონმდებლობით დაკისრებული სხვა უფლებამოსილებების განხორციელება.

მუხლი 10. მონაცემთა დამუშავების სამართლებრივი საფუძვლები

1. პერსონალურ მონაცემთა დამუშავება ხდება შემდეგი საფუძვლებით:

- ა) მონაცემთა სუბიექტმა განაცხადა თანხმობა მის შესახებ მონაცემთა ერთი ან რამდენიმე კონკრეტული მიზნით დამუშავებაზე;
- ბ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტთან დადებული გარიგებით ნაკისრი ვალდებულების შესასრულებლად ან მონაცემთა სუბიექტის მოთხოვნით გარიგების დასადასტურებლად;
- გ) მონაცემთა დამუშავება აუცილებელია დაწესებულებისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად;
- დ) მონაცემთა დამუშავება გათვალისწინებულია კანონით;
- ე) კანონის თანახმად, მონაცემი საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა იგი საჯაროდ ხელმისაწვდომი გახადა;
- ვ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დასაცავად;
- ზ) მონაცემთა დამუშავება აუცილებელია დამუშავებისთვის პასუხისმგებელი პირის ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების დასაცავად, გარდა იმ



შემთხვევისა, თუ არსებობს მონაცემთა სუბიექტის (მათ შორის, არასრულწლოვანის) უფლებების დაცვის აღმატებული ინტერესი;

თ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად).

2. განსაკუთრებული კატეგორიის მონაცემებს დაწესებულება ამუშავებს მხოლოდ იმ შემთხვევაში თუ:

ა) მონაცემები მუშავდება სპეციალური საგანმანათლებლო საჭიროების მქონე პირთა განათლების უფლების რეალიზების მიზნით;

ბ) ნასამართლობისა და ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დამუშავება აუცილებელია შრომითი ვალდებულებისა და ურთიერთობის ხასიათიდან გამომდინარე, მათ შორის დასაქმების თაობაზე გადაწყვეტილების მისაღებად.

3. იმ შემთხვევაში, თუ დაწესებულება მონაცემებს დამუშავებს მონაცემთა სუბიექტის თანხმობით, თანხმობა მხოლოდ იმ შემთხვევაში ჩაითვლება ნამდვილად, თუ ის გაცემულია შესაბამისი ინფორმაციის მიღების შემდეგ, ნებაყოფლობით, მონაცემთა განსაზღვრული და კონკრეტული მიზნით დამუშავებაზე. თანხმობა გაიცემა ნებაყოფლობით და მონაცემთა სუბიექტის აქტიური მოქმედებით.

მუხლი 11. პერსონალურ მონაცემთა დამუშავების პრინციპები

პერსონალურ მონაცემთა დამუშავებისას დაცული უნდა იქნეს შემდეგი პრინციპები:

ა) მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად, მონაცემთა სუბიექტისთვის გამჭვირვალედ და მისი ღირსების შეუღაბავად. მონაცემთა დამუშავების გამჭვირვალობის ვალდებულება არ ვრცელდება ამ კანონით დადგენილ გამონაკლის შემთხვევებზე;

ბ) მონაცემები უნდა შეგროვდეს/მოპოვებული უნდა იქნეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებელი მიზნით;

გ) მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევადაც ისინი მუშავდება;

დ) მონაცემები უნდა იყოს ნამდვილი, ზუსტი და, საჭიროების შემთხვევაში, განახლებული. მონაცემთა დამუშავების მიზნების გათვალისწინებით, არაზუსტი მონაცემები უნდა გასწორდეს, წაიშალოს ან განადგურდეს გაუმართლებელი დაყოვნების გარეშე;

ე) მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან შენახული უნდა იქნეს დეპერსონალიზებული ფორმით, გარდა იმ შემთხვევისა, თუ მონაცემთა დამუშავება განსაზღვრულია კანონით ან/და კანონის



შესაბამისად გამოცემული კანონქვემდებარე ნორმატიული აქტით და მონაცემთა შენახვა აუცილებელი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში აღმატებული ინტერესების დასაცავად;

ვ) მონაცემების უსაფრთხოების დაცვის მიზნით მონაცემთა დამუშავებისას მიღებული უნდა იქნეს ისეთი ტექნიკური და ორგანიზაციული ზომები, რომლებიც სათანადოდ უზრუნველყოფს მონაცემთა დაცვას, მათ შორის, უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვისგან, განადგურებისგან ან/და დაზიანებისგან.

2. თუ მონაცემები უნდა დამუშავდეს მათი შეგროვების/მოპოვების მიზნისგან განსხვავებული მიზნით და დამუშავება მონაცემთა სუბიექტის თანხმობით ან კანონის საფუძველზე არ ხორციელდება, მონაცემთა შეგროვების/მოპოვების მიზნისგან განსხვავებული მიზნით მონაცემთა დამუშავების საკითხის გადაწყვეტისას დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს:

ა) არსებობს თუ არა მონაცემთა შეგროვების/მოპოვების თავდაპირველ მიზანსა და შემდგომ მიზანს შორის კავშირი;

ბ) მონაცემთა შეგროვებისას/მოპოვებისას დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის არსებული ურთიერთობის ხასიათი;

გ) აქვს თუ არა მონაცემთა სუბიექტს მის შესახებ მონაცემთა შემდგომი დამუშავების გონივრული მოლოდინი;

დ) ხორციელდება თუ არა განსაკუთრებული კატეგორიის მონაცემთა დამუშავება;

ე) მონაცემთა სუბიექტისთვის შესაძლო შედეგები, რომლებიც შეიძლება თან ახლდეს მონაცემთა შემდგომ დამუშავებას;

ვ) მონაცემთა ტექნიკური და ორგანიზაციული უსაფრთხოების ზომების არსებობა.

3. მონაცემები, რომლებიც სამართალდამცავმა ორგანომ შეაგროვა თავისი საქმიანობის ფარგლებში, შეიძლება დამუშავდეს დანაშაულებრივი საქმიანობის ზოგადი ანალიზისა და სხვადასხვა გამოვლენილ დანაშაულს შორის კავშირის დადგენის მიზნით.

4. ამ მუხლის პირველი პუნქტის „დ“ ქვეპუნქტით გათვალისწინებული მონაცემთა დამუშავების პრინციპის დაცვის მიზნისთვის დამუშავებისთვის პასუხისმგებელმა პირმა, კონტექსტიდან გამომდინარე, ფაქტებზე დაფუძნებული მონაცემები უნდა განასხვავოს იმ მონაცემებისგან, რომლებიც პირად შეფასებას ეფუძნება. პირად შეფასებაზე დაფუძნებულ მონაცემებთან მიმართებით ამ მუხლის პირველი პუნქტის „დ“ ქვეპუნქტით გათვალისწინებული მონაცემთა დამუშავების პრინციპის ზედმიწევნით დაცვა სავალდებულო არ არის.

5. დამუშავებისთვის პასუხისმგებელი პირის მიერ დანაშაულის თავიდან აცილების (მათ შორის, სათანადო ანალიტიკური კვლევის), დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის, დროებითი მოთავსების იზოლატორში პირის განთავსების უზრუნველყოფის, უკანონო მიგრაციის წინააღმდეგ ბრძოლის, საერთაშორისო დაცვის განხორციელების, ადმინისტრაციულ სამართალდარღვევებზე რეაგირების, სამოქალაქო და სახანძრო უსაფრთხოების უზრუნველყოფის, ოპერატიულ-სამძებრო საქმიანობის, საზოგადოებრივი



უსაფრთხოების ან/და მართლწესრიგის დაცვის (მათ შორის, შესაბამისი სამართალდამცავი ორგანოს ან სასამართლოს მიერ კრიმინოლოგიური კვლევის ჩატარების) მიზნებისთვის მონაცემთა შემდგომი დამუშავება მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებლად არ მიიჩნევა, თუ მონაცემთა დამუშავება გათვალისწინებულია კანონით ან კანონითა და მის საფუძველზე გამოცემული კანონქვემდებარე ნორმატიული აქტით.

6. მონაცემთა შემდგომი დამუშავება საჯარო ინტერესების შესაბამისად არქივირების, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებლად არ მიიჩნევა. ამ პუნქტით გათვალისწინებული მიზნით მონაცემთა ხანგრძლივად შენახვა დასაშვებია, თუ მონაცემთა სუბიექტის უფლებების დასაცავად მიღებულია უსაფრთხოების სათანადო ტექნიკური და ორგანიზაციული ზომები.

7. დამუშავებისთვის პასუხისმგებელი პირი პასუხისმგებელია მონაცემთა დამუშავებისას ამ მუხლით განსაზღვრული პრინციპების დაცვისთვის და მან უნდა შეძლოს მათთან შესაბამისობის დასაბუთება.

მუხლი 12. მონაცემთა სუბიექტის უფლებები

1. მონაცემთა სუბიექტი უფლებამოსილია:

ა) მიიღოს ინფორმაცია მისი მონაცემების დამუშავების შესახებ;

ბ) მიიღოს ინფორმაცია მონაცემების თანადამუშავებლის ან/და უფლებამოსილი პირის შესახებ;

გ) მიიღოს ინფორმაცია მონაცემთა დამუშავების მიზნებზე, საფუძვლებსა და კატეგორიებზე;

დ) მიიღოს ინფორმაცია მონაცემთა იმ მიმღების ვინაობასა ან კატეგორიაზე, რომელსაც გადაეცა ან მომავალში გადაეცემა მონაცემები;

ე) მიიღოს ინფორმაცია მონაცემთა შენახვის ვადაზე, ან თუ კონკრეტული ვადის განსაზღვრა შეუძლებელია, ვადის განსაზღვრის კრიტერიუმებზე;

ვ) მიიღოს ნებისმიერი ხელმისაწვდომი ინფორმაცია მონაცემთა შეგროვების წყაროს შესახებ, თუ მონაცემთა შეგროვება არ ხდება უშუალოდ მონაცემთა სუბიექტისაგან;

ზ) მოითხოვოს მონაცემთა გაცნობა და ასლის მიღება;

თ) მოითხოვოს მის შესახებ დამუშავებული მცდარი/არაზუსტი მონაცემების დაუყოვნებლივ გასწორება, განახლება, გადატანა ან მონაცემთა დამუშავების მიზნების გათვალისწინებით, არასრული მონაცემების შევსება, მათ შორის, დამატებითი ცნობის/დოკუმენტის წარდგენის გზით;

ი) მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, მონაცემთა წაშლა ან მონაცემთა განადგურება თანხმობის გამოთხოვით;

კ) მოითხოვოს მონაცემთა დაბლოკვა.



2. აღნიშნული უფლებებით სარგებლობისათვის მონაცემთა სუბიექტი უნდა დაუკავშირდეს დამუშავებაზე უფლებამოსილ პირს ან დამუშავებისათვის პასუხისმგებელ პირს, იმ შემთხვევაში, თუ მონაცემები მასთან ინახება.

2¹. იმის შესახებ, თუ ვინ ახორციელებს მონაცემების შენახვასა და მონაცემთა სუბიექტის ზემოაღნიშნული უფლებების ფარგლებში განხორციელებულ მომართვაზე რეაგირებას, სკოლისა და კონკრეტულ კლიენტ ორგანიზაციას შორის ურთიერთობის ფარგლებში, მონაცემთა სუბიექტი ინფორმირებულია პოლიტიკის შესაბამისად.

3. მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში სკოლა ვალდებულია მოთხოვნის თაობაზე შეტყობინების მიღებიდან არაუგვიანეს 10 (ათი) სამუშაო დღისა უზრუნველყოს მონაცემთა სუბიექტისათვის შესაბამისი ინფორმაციის მიწოდება. ეს ვადა განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით შეიძლება გაგრძელდეს არაუმეტეს 10 სამუშაო დღით, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ უნდა ეცნობოს.

4. მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. თანხმობის გამოხმობა შესაძლებელია იმავე ფორმით, როგორც მისი გაცემა.

5. მონაცემთა სუბიექტის უფლებები შეიძლება შეიზღუდოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებულ შემთხვევებში და წესით.

6. იმ შემთხვევაში, როდესაც მონაცემთა სუბიექტის უფლებების რეალიზებისათვის განსახორციელებელი ქმედებები მონაცემთა დამუშავების პროცესში ჩართული სხვა უწყებების, მაგ, პერსონალურ მონაცემთა დაცვის სამსახურის, უფლებამოსილებებს განეკუთვნება, დაწესებულება უფლებამოსილია აღნიშნული წერილობით განუმარტოს მონაცემთა სუბიექტს.

7. მონაცემთა სუბიექტი სარგებლობს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით გათვალისწინებული სუბიექტის ყველა სხვა უფლებით.

8. პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებულ ნებისმიერ საკითხზე მონაცემთა სუბიექტი უფლებამოსილია, მიმართოს სკოლის დირექტორს ან/და პერსონალურ მონაცემთა დაცვის ოფიცერს.

9. პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე დაცვის შემთხვევაში მონაცემთა სუბიექტს უფლება აქვს კანონმდებლობით დადგენილი წესით, მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს ან/და სასამართლოს.

მუხლი 13. მონაცემებზე წვდომა

1. თანამშრომლებს წვდომა აქვთ მხოლოდ იმ მონაცემებზე და იმ ფარგლებში, რაც აუცილებელია მათი მოვალეობების შესასრულებლად. თანამშრომლის შვებულების ან სხვა მიზეზით მოვალეობის შესრულების შემთხვევაში მოვალეობის შემსრულებელს აქვს წვდომა ასევე იმ პირის წვდომის ფარგლებში, ვის მოვალეობასაც ასრულებს, მოვალეობის შესრულების ბრძანებაში განსაზღვრულ ფარგლებში და წესით.

3. <https://portal.emis.ge/my.policy> (eSchool) წვდომა აქვს:

ა) საქმისმწარმოებელს - სრული წვდომა;



ბ) ხარისხის ჯგუფს - სრული წვდომა;

გ) დირექტორს - სრული წვდომა;

დ) IT მენეჯერს - სრული წვდომა;

ე) მასწავლებელს - შეზღუდული წვდომა;

4. <https://eservices.schoolbook.ge/> (ელექტრონული ჟურნალი) წვდომა აქვს:

ა) ხარისხის ჯგუფს - სრული წვდომა;

ბ) სასწავლო ნაწილს - სრული წვდომა;

გ) მასწავლებელს - შეზღუდული წვდომა;

დ) მშობელს/კანონიერ წარმომადგენელს - შეზღუდული წვდომა;

ე) მოსწავლეს - შეზღუდული წვდომა.

5. დასაქმებულებთან მონაცემებზე წვდომის უფლება აქვთ:

ა) საქმისმწარმოებელს - სრული წვდომა;

ბ) ხარისხის ჯგუფს - სრული წვდომა;

გ) დირექტორს - სრული წვდომა;

დ) IT მენეჯერს - სრული წვდომა;

ე) ფსიქოლოგს - შეზღუდული წვდომა;

ვ) ექთანს - შეზღუდული წვდომა.

6. მოსწავლეთა პერსონალურ მონაცემებზე წვდომის უფლება აქვთ:

ა) საქმისმწარმოებელს - სრული წვდომა;

ბ) ხარისხის ჯგუფს - სრული წვდომა;

გ) დირექტორს - სრული წვდომა;

დ) IT მენეჯერს - სრული წვდომა;

ე) ფსიქოლოგს - შეზღუდული წვდომა;

ვ) ექთანს - შეზღუდული წვდომა;

ზ) მასწავლებელს - შეზღუდული წვდომა.

5. კოლეგიური ორგანოების სხდომის ოქმებზე წვდომის უფლება აქვს დირექტორს, საქმისმწარმოებელს, სასწავლო ნაწილს და ხარისხის ჯგუფის წევრებს, მათი აღრიცხვისა და შენახვის მიზნით.

6. დოკუმენტბრუნვის სისტემაზე და მასში არსებულ ინფორმაციაზე:



- ა) სრული წვდომის უფლება აქვს - დირექტორს შემოსული კორესპონდენციის განაწილებისა და სათანადო რეაგირების უზრუნველყოფის მიზნით;
- ბ) შეზღუდული წვდომის უფლება აქვთ - სხვა დასაქმებულებს მათზე განაწილებული კორესპონდენციის განხილვისა და შესაბამისი პასუხების მომზადების მიზნით.

მუხლი 14. მონაცემთა უსაფრთხოება და თანამშრომელთა ვალდებულებები

1. სკოლა სათანადო, ორგანიზაციული და ტექნიკური ზომების მიღებით უზრუნველყოფს მონაცემთა უსაფრთხოებას, მათ დაცვას შემთხვევითი ან უკანონო განადგურებისგან, შეცვლისაგან, გამჟღავნებისგან, მოპოვებისგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან.
2. სკოლა ვალდებულია მონაცემთა სუბიექტს დეტალურად აცნობოს ინფორმაცია იმის შესახებ, თუ რა მონაცემებს აგროვებს, როგორ იყენებს მათ, ვის გადასცემს და როგორ იცავს მონაცემთა უსაფრთხოებას.
3. სკოლაში დასაქმებული ნებისმიერი პირი, რომელიც მონაწილეობს მონაცემთა დამუშავებაში ან რომელსაც აქვს მონაცემებზე წვდომა, ვალდებულია:
 - ა) არ გასცდეს მისთვის მინიჭებული უფლებამოსილების ფარგლებს;
 - ბ) დაიცვას მონაცემთა საიდუმლოება და კონფიდენციალურობა, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემდეგ;
 - გ) არ გამოიყენოს მონაცემები პირადი, არასამსახურებრივი მიზნებისთვის;
 - დ) არ გახადოს მონაცემები ხელმისაწვდომი არაუფლებამოსილი პირებისათვის, მათ შორის მონაცემთა უყურადღებოდ დატოვების და/ან არაუფლებამოსილი პირების თანდასწრებით განხილვის გზით.
- 3¹. წინამდებარე დოკუმენტით დადგენილი წესების დარღვევა წარმოადგენს სკოლის შრომის შინაგანაწესის დარღვევას და შესაძლოა ითვალისწინებდეს შესაბამის დისციპლინურ ზომას.
4. მონაცემებზე წვდომა აქვთ მხოლოდ იმ თანამშრომლებს და იმ მოცულობით, რომელთაც მონაცემები სჭირდებათ საკუთარი ფუნქცია-მოვალეობების შესასრულებლად.
5. სკოლის მიერ გამოყენებულ ელექტრონულ სისტემებზე წვდომა შესაძლებელია მხოლოდ ინდივიდუალური მომხმარებლის სახელისა და რთული კომბინაციის შემცველი პაროლის საშუალებით, რომელიც პერიოდულად ახლდება. აკრძალულია მომხმარებლის სახელისა და პაროლის ვინმესთვის გამჟღავნება/სარგებლობაში გადაცემა.
6. ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული მოქმედებები აღირიცხება/ლოგირდება შესაბამის ელექტრონულ ჟურნალებში. არაელექტრონული ფორმით არსებულ მონაცემთა დამუშავებისას დაწესებულების დასაქმებული შესაბამისი პირ(ებ)ი ვალდებული არიან უზრუნველყონ მონაცემთა გამჟღავნებასთან ან/და ცვლილებასთან დაკავშირებული ყველა მოქმედების (მათ შორის, ინციდენტების შესახებ ინფორმაციის) აღრიცხვა.



7. მონაცემები ინახება სკოლის დაცულ სერვერზე, რომელიც განთავსებულია საქართველოში. დაცვის მექანიზმებიდან სკოლა იყენებს “FIREWALL” სისტემას. სერვერზე წვდომა აქვს IT მენეჯერს.

9. სკოლის მიერ გამოყოფილია ცალკე სპეციალურად დაცული სივრცე, რომელშიც ინახება დაარქივებული სახით მონაცემები. აღნიშნულ სივრცეში შესვლა ხდება სპეციალური ავტორიზაციით და ხდება აღრიცხვა.

10. განსაკუთრებული კატეგორიის მონაცემებიდან, როგორცაა ჯანმრთელობაზე ინფორმაცია, ინახება ექიმის კაბინეტში და მათზე წვდომა ხდება მხოლოდ ავტორიზებული პირების მიერ. გათვალისწინებულია უსაფრთხოებისა და წვდომაზე აღრიცხვის სისტემა.

11. სკოლა შეიმუშავებს მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტს, რომელიც მოიცავს: მონაცემთა კატეგორიის, მათი დამუშავების მიზნების, პროპორციულობის, პროცესისა და საფუძვლების აღწერას; ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის შესაძლო საფრთხეების შეფასებას და მონაცემთა უსაფრთხოების დაცვის მიზნით გათვალისწინებული ორგანიზაციულ-ტექნიკური ზომების აღწერას.

მუხლი 15. მონაცემთა შენახვის ვადები

1. სკოლა ინახავს მხოლოდ იმ მონაცემებს, რომლებიც აუცილებელია მონაცემთა დამუშავების კონკრეტული, კანონიერი მიზნის მისაღწევად.

2. განსაკუთრებული კატეგორიის მონაცემები ინახება როგორც ავტომატური და არაავტომატური საშუალებებით იმ ვადით, რომლითაც მიიღწევა ლეგიტიმური მიზანი პერსონალურ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისა და მონაცემთა სუბიექტებისთვის გათვალისწინებული საფუძვლით.

3. მონაცემები ინახება კანონმდებლობით განსაზღვრული ვადების შესაბამისად. მონაცემთა შენახვის ვადებისა და წესის განსაზღვრის საჭიროების შემთხვევაში, სკოლა ითვალისწინებს პერსონალურ მონაცემთა დამუშავების პრინციპებს.

4. სკოლაში მონაცემთა მატერიალური ფორმით შენახვისათვის დადგენილია შემდეგი ვადები:

ა) მოსწავლის პირადი საქმეები ინახება 75 ვადით;

ბ) თანამშრომელთა პირადი საქმეები ინახება 75 ვადით;

გ) თანამშრომელთა სამუშაო დროის აღრიცხვის ფორმები ინახება 1 წლის ვადით;

დ) კოლეგიური ორგანოების სხდომის ოქმები ინახება 1 წლის ვადით;

ე) CV (რეზიუმე) 1 წლის ვადით.

5. მატერიალური ფორმით არსებული დოკუმენტაცია (მიმდინარე დოკუმენტები, აქტიური პირადი საქმეები) ინახება სამასწავლებლო ოთახში მდებარე კარადებში. დოკუმენტებზე და/ან მათში დაცულ ინფორმაციაზე წვდომა შესაძლებელია მხოლოდ საქმისმწარმოებლისგან აღნიშნული დოკუმენტაციის მიღების და შესაბამისი აღრიცხვის გზით.



6. მატერიალური ფორმით არსებული დოკუმენტაცია (პირადი საქმეები, კოლეგიური ორგანოების სხდომის ოქმები), რომელიც არ არის აქტიურ მოხმარებაში, არქივდება და ინახება სპეციალურად გამოყოფილ ოთახში. ოთახი იკეტება გასაღებით, რომელიც ინახება საქმისმწარმოებელთან. დაარქივებულ დოკუმენტებზე წვდომა შესაძლებელია დირექტორის ნებართვით, შესაბამისი წერილობითი საფუძვლის არსებობისას.

7. შენახვის ვადის გასვლის შემდეგ მატერიალური ფორმით არსებული დოკუმენტები ნადგურდება, რის შესახებაც დგება შესაბამისი აქტი.

მუხლი 16. მონაცემთა გადაცემა/გამჟღავნება

1. დაწესებულების მიერ დამუშავებული მონაცემები სამართლებრივი საფუძვლის არსებობის შემთხვევაში კანონმდებლობით დადგენილი წესითა და მოცულობით შეიძლება გადაეცეს შემდეგ მესამე პირებს:

ა) სამართალდამცავ ორგანოებს;

ბ) სასამართლოს;

გ) პერსონალურ მონაცემთა დაცვის სამსახურს;

დ) კანონმდებლობით დადგენილ სხვა გათვალისწინებულ ორგანოებს.

2. მონაცემი შესაძლოა ასევე გადაეცეს:

ა) განათლების, მეცნიერების და ახალგაზრდობის სამინისტროს;

ბ) ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს;

გ) აჭარის ავტონომიური რესპუბლიკის განათლების, კულტურისა და სპორტის სამინისტროს;

დ) აჭარის ავტონომიური რესპუბლიკის ჯანმრთელობის და სოციალური დაცვის სამინისტროს;

ე) ბათუმის მერია;

ვ) დაცვის სამსახურს.

3. სკოლა იყენებს მესამე პირს მომსახურების გაწევის პროცესში დახმარების, შიდა ინფორმაციული ტექნოლოგიების სისტემების გამართული მუშაობისა და მართვისათვის;

4. ამ მუხლის პირველი და მეორე პუნქტებით გათვალისწინებულ შემთხვევებში ინფორმაციის გამჟღავნებისას სკოლა აღრიცხავს, თუ რომელი მონაცემი იქნა გამჟღავნებული, ვისთვის, როდის და რა სამართლებრივი საფუძვლით. აღნიშნული ინფორმაცია ინახება სუბიექტის შესახებ მონაცემებთან ერთად მათი შენახვის ვადის განმავლობაში.

მუხლი 17. ვიდეომონიტორინგი



1. სკოლა ვიდეომონიტორინგის სისტემას იყენებს კანონით დაკისრებული ვალდებულებების შესასრულებლად - პირის უსაფრთხოებისა და საკუთრების დაცვის, აგრეთვე, არასრულწლოვანთა მავნე ზეგავლენისაგან დაცვის მიზნებისთვის.
2. მონაცემთა დამუშავების შესახებ მონაცემთა სუბიექტების ინფორმირების მიზნით შენობაში თვალსაჩინო ადგილებში განთავსებულია შესაბამისი გამაფრთხილებელი ნიშნები.
3. სკოლა უზრუნველყოფს იმ თანამშრომელთა სათანადო წესით ინფორმირებას, რომელთა სამუშაო სივრცეც ექვევს ვიდეომონიტორინგის სისტემის ხედვის არეალში.
4. ვიდეო მონიტორინგის სისტემა და ჩანაწერები დაცულია არამართლზომიერი წვდომისა და გამოყენებისაგან. მასზე წვდომები დაცულია მომხმარებლის სახელითა და პაროლით.
5. ვიდეო მონიტორინგის სისტემა დაცულია შიფრაციის ფუნქციით და აღჭურვილია შესაბამისი თვითგანადგურების მექანიზმით. შემუშავებულია ვიდეო მონიტორინგით მოპოვებულ მონაცემებზე წვდომის ავტორიზაციის მქონე პირთა წრე, რომელსაც წარმოადგენს:
 - ა) IT მენეჯერი - **სრული წვდომა;**
 - ბ) დირექტორის მოადგილეს სამეურნეო დარგში და უსაფრთხოებაზე პასუხისმგებელ პირს - **სრული წვდომა;**
 - ბ) ხარისხის ჯგუფს - **სრული წვდომა;**
 - ბ) დაცვის სამსახურს - **შეზღუდული წვდომა.**
6. ვიდეო მონიტორინგით მოპოვებული მონაცემების შენახვის ვადაა 30 კალენდარული დღე, რის შემდეგაც, მონაცემები სისტემის მიერ ავტომატურად ნადგურდება.
7. ვიდეო მონიტორინგის არეალი მოიცავს:
 - ა) დაწესებულების საერთო არეალს;
 - ბ) დერეფნებს;
 - გ) კიბეებს;
 - დ) ლიფტებს;
 - დ) სპორტდარბაზს;
 - ე) დაწესებულების გარე პერიმეტრს, რომელშიც შედის - დაწესებულების გარე სივრცე, ჭიშკრები, ღობეები, შემოსასვლელი, ავტოსადგომი.
8. ვიდეო მონიტორინგი არ ხორციელდება გამოსაცვლელ ოთახებში, ჰიგიენისთვის განკუთვნილ ადგილებში ან ისეთ სივრცეში, სადაც სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს ან/და ვიდეო მონიტორინგის განხორციელება საყოველთაოდ აღიარებულ ზნეობრივ ნორმებს ეწინააღმდეგება.

მუხლი 18. ვიდეო სამეთვალყურეო სისტემაზე წვდომის კონტროლი



სკოლის საკუთრებაში არსებული ვიდეო სამეთვალყურეო სისტემის ფარგლებში განსაზღვრულია შემდეგი ტიპის წვდომები:

ა) ვიდეომონიტორინგის კამერების მონიტორინგი რეალურ (online) რეჟიმში - აღნიშნული წვდომის მქონე მომხმარებელს შეუძლია მხოლოდ თვალყურის ადევნოს მიმდინარე კადრებს. შეზღუდული აქვს ჩანაწერის გადახვევის და გადმოწერის (კომპიუტერზე ან ინფორმაციის სხვა მედია მატარებელზე) უფლება;

ბ) ვიდეომონიტორინგის კამერების ჩანაწერების გადახვევის და თვალყურის დევნების უფლება - აღნიშნული წვდომის მქონე მომხმარებელს შეუძლია როგორც კამერების რეალურ რეჟიმში მონიტორინგი, ასევე, ჩანაწერების გადახვევა და თვალყურის დევნება, მაგრამ შეზღუდული აქვს ჩანაწერის გადმოწერის (კომპიუტერზე ან ინფორმაციის სხვა მედია მატარებელზე) უფლება;

გ) ვიდეომონიტორინგის კამერების ჩანაწერების გადმოწერა - აღნიშნული წვდომის მქონე მომხმარებელს შეუძლია კამერების რეალურ რეჟიმში მონიტორინგი, ჩანაწერების გადახვევა და თვალყურის დევნება, ჩანაწერების გადმოწერა ლოკალურ ქსელში და შესაბამისი დასტურის შემთხვევაში უფლებამოსილი პირისთვის მიწოდება;

დ) ტექნიკური მხარდაჭერის უფლება - აღნიშნული წვდომის მქონე მომხმარებელს აქვს ვიდეო სამეთვალყურეო სისტემაში ახალი მომხმარებლების შექმნის, არსებული მომხმარებლების გაუქმების, ვიდეო სამეთვალყურეო სისტემაში არსებული ელექტრონულად შესრულებული მოქმედებების (ლოგების) მონიტორინგის, ტექნიკური პრობლემების შემთხვევაში ხარვეზის აღმოსაფხვრელად სხვადასხვა ქმედებების განხორციელების, ასევე კონფიგურაციების ცვლილებების განხორციელების უფლება.

შენიშვნა: მომხმარებელი არის ნებისმიერი პირი რომელსაც აქვს წვდომა ვიდეო სამეთვალყურეო სისტემაზე. ვიდეო სამეთვალყურეო სისტემაზე წვდომა წარმოებს მხოლოდ ინდივიდუალური მომხმარებლის სახელისა და პაროლის საშუალებით.

მუხლი 19. პერსონალურ მონაცემთა დაცვის ოფიცერი

1. სკოლას ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც უზრუნველყოფს პერსონალურ მონაცემთა დამუშავების პროცესების შესაბამისობას პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან.

2. პერსონალურ მონაცემთა დაცვის ოფიცერი:

ა) აკონტროლებს სკოლაში პერსონალურ მონაცემთა დამუშავების პროცესს;

ბ) მონაწილეობს მონაცემთა დამუშავების რისკების შეფასების პროცესში საჭიროების შემთხვევაში;

გ) თანამშრომლობს პერსონალურ მონაცემთა დაცვის სამსახურთან საჭიროების შემთხვევაში;

დ) უზრუნველყოფს თანამშრომელთა ინფორმირებასა და გადამზადებას პერსონალურ მონაცემთა დაცვის საკითხებთან დაკავშირებით;

ე) განიხილავს მონაცემთა სუბიექტის განცხადებებს, საჩივრებს ან/და მომართვებს;



ვ) პერსონალურ მონაცემთა დაცვის საკითხზე კონსულტაციას უწევს სკოლაში დასაქმებულ პირებს;

ზ) აწარმოებს და პერსონალურ მონაცემთა დაცვის სამსახურს წარუდგენს ფაილური სისტემების კატალოგებს;

თ) ავლენს, შეისწავლის და სათანადო რეაგირებას ახდენს პერსონალურ მონაცემთა დარღვევის ფაქტებზე;

ი) პერსონალურ მონაცემთა დაცვის საკითხების ეფექტიანად უზრუნველსაყოფად ახორციელებს კანონმდებლობით, მათ შორის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, მისთვის დაკისრებულ სხვა უფლება - მოვალეობებს.

მუხლი 20. პოლიტიკის განახლება და დამატებითი ინფორმაცია

მონაცემთა დამუშავებასთან დაკავშირებული ცალკეული საკითხების ცვლილების შემთხვევაში, პოლიტიკა ექვემდებარება საჭიროებისამებრ განახლებას.