შპს ზოგადსაგანმანათლებლო სკოლა

„ინტელექტ-პლიუსის“

ინფორმაციული უსაფრთხოების დაცვის წესი

თბილისი, 2025

მუხლი 1. პრეამბულა

1. შპს „ზოგადსაგანმანათლებლო სკოლა ინტელექტ-პლიუსი“ (შემდგომში „სკოლა“) წარმოადგენს ზოგადსაგანმანათლებლო დაწესებულებას, რომელიც საკუთარი ფუნქციების შესასრულებლად ამუშავებს მოსწავლეების, მოსწავლეების მშობლის/კანონიერი წარმომადგენლის, მასწავლებლებისა და სხვა თანამშრომლების პერსონალურ მონაცემებს. საკუთარი უფლებამოსილებების განსახორციელებლად, სკოლა ამუშავებს, როგორც ჩვეულებრივ, ისე განსაკუთრებული კატეგორიის მონაცემებს. მოსწავლეთა მონაცემების დამუშავება იწყება მათი სკოლაში რეგისტრაციის შედეგად და გრძელდება მთელი სასწავლო პროცესის მანძილზე. მოსწავლის შესახებ დამუშავებული მონაცემები მოიცავს ინფორმაციას მოსწავლის, ასევე მათი მშობლების/კანონიერი წარმომადგენლების შესახებ პირადი მონაცემების, მოსწავლის სკოლაში სწავლის განმავლობაში მისი შეფასებისა და აქტიურობის შესახებ. ზოგადი განათლების უზრუნველყოფის მიზნებისათვის მონაცემთა დამუშავების პროცესში სკოლა ერთიანი სისტემის ნაწილია, რომელშიც ჩართულია საქართველოს განათლებისა და მეცნიერების სამინისტრო და მის დაქვემდებარებაში არსებული საჯარო სამართლის იურიდიული პირები, რომლებიც საკუთარი უფლებამოსილებების ფარგლებში განსაზღვრავენ მონაცემთა დამუშავების ფორმასა და მიზნებს. ამრიგად, სკოლაში მონაცემები მუშავდება როგორც ელექტრონული პლატფორმების, ასევე - ქაღალდურ მატარებლებზეც. პერსონალური მონაცემების დაცვა სასკოლო საზოგადოების ყველა წევრის უფლებაა, შესაბამისად მონაცემთა დამუშავება მკაფიოდ რეგლამენტირებული პროცესია და სკოლა უზრუნველყოფს ყველა წევრის პერსონალური მონაცემების დაცვას, რისთვისაც სკოლას შემუშავებული აქვს პერსონალურ მონაცემთა დამუშავების წესი და განსაზღვრული ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი.
2. სკოლის მიერ პერსონალურ მონაცემთა დამუშავების წესი (შემდგომში „წესი“), რომელიც გამოქვეყნებულია საჯაროდ ოფიციალური ვებ-გვერდის საშუალებით, გამოიყენება სკოლის მიერ მოსწავლეების, მოსწავლეების მშობლების/კანონიერი წარმომადგენლების, მასწავლებლებისა და სხვა დასაქმებული თანამშრომლების მონაცემთა დამუშავების პროცესში და ვრცელდება სკოლის მიერ მონაცემების ნებისმიერი ფორმით დამუშავებაზე.
3. წინამდებარე წესი, რომელიც ეხება ინფორმაციულ უსაფრთხობას, შემუშავებულია “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის, “ზოგადი განათლების შესახებ” საქართველოს კანონისა და სხვა მარეგულირებელი აქტების საფუძველზე.

მუხლი 2. ზოგადი დებულებები

1. ინფორმაციული უსაფრთხოების წესი არეგულირებს სკოლაში პერსონალური მონაცემების უსაფრთხოების დაცვის მიზნით შესაბამისს გასატარებელ ღონისძიებებს და რეგულაციებს, რომელიც სკოლის მიერ დაცულია პერსონალური მონაცემების უსაფრთხოდ და კანონის შესაბამისად დაცვის მიზნით.

მუხლი 3. ტერმინთა განმარტება

1. **“სკოლა”** - შპს ზოგადსაგანმანათლებლო სკოლა ინტელექტ-პლიუსი
2. **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.

3. **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.
4. **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.
5. **მონაცემთა სუბიექტი** – ნებისმიერი ფიზიკური პირი, რომლის შესახებ მონაცემიც მუშავდება.
6. **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.
7. **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.
8. **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.
9. **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.
10. **მონაცემთა მიმღები-** ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელსაც მონაცემები გადაეცა, გარდა პერსონალურ მონაცემთა დაცვის სამსახურისა.
11. **მესამე პირი-** ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, გარდა მონაცემთა სუბიექტისა, პერსონალურ მონაცემთა დაცვის სამსახურისა, დამუშავებისთვის პასუხისმგებელი პირისა, დამუშავებაზე უფლებამოსილი პირისა, სპეციალური წარმომადგენლისა და იმ პირისა, რომელიც უფლებამოსილია დაამუშაოს მონაცემები

დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის პირდაპირი დავალებით.

12. წინამდებარე მუხლით გათვალისწინებული ტერმინების გარდა, ამ წესში გამოყენებულ ტერმინებს აქვთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მნიშვნელობა.

მუხლი 4. ინფორმაციული უსაფრთხოების დაცვის ღონისძიებები

1. სკოლა უზრუნველყოფს ინფორმაციული უსაფრთხოების დაცვას, რომელიც პირველრიგში ხორციელდება თითოეული დასაქმებულისათვის სპეციალურად შექმნილი ანგარიშის საშუალებით, რომლის გამოყენებითაც, თითოეულ დასაქმებულს წვდომა აქვს მხოლოდ მისთვის განკუთვნილ პერსონალურ მონაცემებზე.
2. სკოლაში თითოეული დასაქმებული ინფორმირებულია იმის, შესახებ რომ მათ მიერ გამოყენებული კომპიუტერული სისტემაში დაშვების პაროლი უნდა იქნას მინიმუმ 6 ნიშნა, უნდა შეიცავდეს სხვადასხვა ნიშნებსა და სიმბოლოებს და უნდა იცვლებოდეს 3 (სამი) თვეში ერთხელ.
3. სკოლის თითოეულ მასწავლებელს, მხოლოდ წვდომა აქვს მისთვის განკუთვნილი ელექტრონულ ჟურნალში არსებულ ინფორმაციაზე, რომელიც განაწილებულია იმის მიხედვით თუ რომელ საგანს კითხულობს მასწავლებელი. ამასთან, დამრიგებელს წვდომა აქვს მხოლოდ მისთვის განკუთვნილი სადამრიგებლო კლასის მოსწავლეების პერსონალურ მონაცემებზე.
4. სკოლის ოფიციალური ვებ-გვერდი მომზადებულია უსაფრთხო სისტემების საშუალებით, რომელიც უზრუნველყოფს არაავტორიზებული პირების მხრიდან ვებ-გვერდზე შეღწევის ამოცნობას. უსაფთხოების სისტემა სკოლის მიერ წელიწადში ერთხელ ექვემდებარება განახლებასა და პერიოდულ შემოწმებას.
5. სკოლას, იმისათვის რომ ინფორმაცია მუდვიმად შენახული და დაცული იყოს გამოყენებული აქვს ელექტრონული ღრუბელი (ე.წ. cloud), რომელზეც თითოეულ დასაქმებულს პირდაპირ გადააქვს მათ მიერ მომზადებული დოკუმენტაცია/ინფორმაცია. აღნიშნული ელექტრონული ღრუბელი არის ერთი ტერაბაიტის შემცველი მოცულობისა და საჭიროების შემთხვევაში (თუ მოცულობა შეივსება) ექვემდებარება მოცულობის გაზრდას.
6. წინამდებარე მუხლის მე-5 პუნქტით გათვალისწინებული ელექტრონულ ღრუბელზე (ე.წ. cloud) არსებული დოკუმენტაციაზე/ინფორმაციაზე წვდომა თითოეულ დასაქმებულს აქვს მხოლოდ მისი პოზიციის შესაბამისად გათვალისწინებულ ინფორმაციაზე. აღნიშნულ ელექტრონულ ღრუბელზე (ე.წ.cloud) ინფორმაცია სრულად ხილულია მხოლოდ სკოლის დირექტორისათვის, რომელსაც შეუძლია ნებისმიერი დასაქმებულის მიერ ატვირთული ინფორმაცია/დოკუმენტაცია იხილოს და შეამოწმოს.
7. წინამდებარე მუხლის მე-5 პუნქტისაგან განსხვავებით, იმისათვის რომ პერსონალური მონაცემები, დოკუმენტაცია და ინფორმაცია ექვემდებარებოდეს მუდვიმად შენახვას, არაავტორიზებული პირებისაგან წვდომის შეზღუდვასა და დაცვას, სკოლის თითოეულ დასაქმებულს გარდა, ელექტრონულ ღრუბელში გადატანილი ინფორმაციისა, 3 (სამი) თვეში ერთხელ წინასწარ შეძენილ 1 (ერთი) ტერაბაიტის მოცულობის სამახსოვრო ბარათზე გადააქვს მის მიერ, მის დაქვემდებარებაში არსებული ინფორმაცია/დოკუმენტაცია, რომელზეც წვდომის უფლება აქვს მხოლოდ სკოლის დირექტორს. აღნიშნული სამახსოვრო ბარათი ინახება სკოლის დირექტორის მიერ.

8. თითოეული დასაქმებულისათვის და სკოლის მასწავლებლებისათვის პერიოდულად, სკოლა უზრუნველყოფს ტრენინგის ჩატარებას პერსონალური მონაცემების დაცვის, ინფორმაციული უსაფრთხოებისა და მისი დაცვის შესახებ.
9. სკოლის ტერიტორიაზე დაშვება ხდება მხოლოდ უფლებამოსილი პირებისათვის. სკოლას შესასვლელში აქვს დაცვის ოთახი, რომელიც თითოეული არაუფლებამოსილი პირის აღრიცხვას აწარმოებს, ადგენს სკოლაში შესვლის მიზნობრიობასა და აღნიშნულის შემდეგ იღებს გადაწყვეტილებას სკოლის ტერიტორიაზე მისი დაშვების შესახებ.
10. ინფორმაციული უსაფრთხოების დაცვის მიზნით, სკოლის მიერ შემუშავებული "პერსონალური მონაცემების დაცვის სახელმძღვანელო პრინციპების" შესახებ წესის შესაბამისად, ახორციელებს ვიდეომონიტორინგს, რომლის შესახებაც გამაფრთხილებელი ნიშანია გამოკრული სკოლის მთელ ტერიტორიაზე.

მუხლი 5. დამატებითი დებულებები

1. წინამდებარე წესი ძალაში შედის დირექტორის ბრძანებით დამტკიცების შემდეგ.
2. წინამდებარე წესის ძალაში შესვლისთანავე უქმდება, სკოლაში ამ დოკუმენტის ძალაში შესვლამდე მოქმედი ამ წესით გათვალისწინებული საკითხების მარეგულირებელი დებულება/წესი.
3. სკოლის მოსწავლეები, თანამშრომლები და სკოლის შენობაში/შიდა ტერიტორიაზე მყოფი პირები ვალდებულნი არიან გაეცნონ წინამდებარე დოკუმენტს, ადმინისტრაცია ვალდებულია ნებისმიერ დროს მისცეს მათ წინამდებარე დოკუმენტის გაცნობის შესაძლებლობა;
4. ყველა საკითხი, რომელიც არ არის გათვალისწინებული წინამდებარე დოკუმენტით და სკოლაში მოქმედი სხვა მარეგულირებელი დებულებებით/წესებით, რეგულირდება საქართველოს კანონმდებლობით;
5. წინამდებარე დოკუმენტი ძალას კარგავს მისი გაუქმების, ახალი "ინფორმაციული უსაფრთხოების დაცვის წესის" ან წინამდებარე დოკუმენტში გათვალისწინებული საკითხების მომწესრიგებელი ახალი დოკუმენტ(ებ)ის ამოქმედების დღიდან.