

БЕКІТЕМІН

Қостанай облысы әкімдігі білім
басқармасының

«Қостанай педагогикалық
колледжі» КМҚК директоры

Г.У. Уразамбетова

«27» _____ 2021 год

**Қостанай облысы әкімдігінің білім басқармасы
«Қостанай педагогикалық колледжі» КМҚК
ақпараттық қауіпсіздік саясаты туралы ереже**

1. Кіріспе

1.1. Қостанай облысы әкімдігі білім басқармасының "Қостанай педагогикалық колледжі". КМҚК ақпараттық қауіпсіздік туралы ережесі (бұдан әрі – Ереже) Ақпараттық-коммуникациялық технологиялар саласында орындалуы міндетті талаптарды белгілеуді қамтамасыз ету және колледждің ақпараттық қауіпсіздігін қамтамасыз ету мақсатында әзірленді.

1.2. Ережеде келесі ұғымдар қолданылады:

Сервер-пайдаланушылардың сұраныстарын сақтау және өңдеу функцияларын орындайтын және колледждің ақпараттық жүйесінің сенімділігін, дайындық дәрежесін және қауіпсіздік шараларын қамтамасыз ету бойынша жоғары талаптарға байланысты пайдаланушылардың жергілікті қолжетімділігіне (бөлінген сервер, жүру және басқа да мамандандырылған құрылғылар) арналмаған аппараттық-бағдарламалық кешен.

Жұмыс станциясы – Қостанай облысы әкімдігі білім басқармасының "Қостанай педагогикалық колледжі" КМҚК (бұдан әрі-колледж) автоматтандырылған жүйесінің ресурстарына пайдаланушылардың қол жеткізуіне, ақпаратты қабылдау-беру мен өңдеуге арналған дербес компьютер (терминал).

Бағдарламалық қамтамасыз ету бойынша маман-лауазымды тұлға, оның міндеттеріне қызмет көрсету, барлық аппараттық-бағдарламалық кешенін колледж, желілік ресурстарға қол жеткізуді басқару, сондай-ақ қолдау талап етілетін деңгейін істен шығуының тұрақтылығы мен деректердің қауіпсіздігі, олардың резервтік көшіру және қалпына келтіру.

Пайдаланушы-лауазымдық міндеттерін орындау үшін колледждің ақпараттық жүйесінің ресурстарын пайдаланатын колледж қызметкері.

Есептік жазба-желілік пайдаланушы туралы ақпарат: пайдаланушы аты, оның паролі, жүйеде жұмыс істеу кезінде ресурстарға қол жеткізу құқығы және артықшылықтары. Есептік жазбада қосымша ақпарат болуы мүмкін (электрондық пошта мекенжайы, телефон және т.б.).

Пароль-пайдаланушы компьютерлік жүйеге деректер мен бағдарламаларға қол жеткізу үшін ұсынатын таңбалардың (әріптер, сандар, арнайы таңбалар) құпия жолы. Пароль деректерді рұқсатсыз кіруден қорғау құралы болып табылады.

Өкілеттікті өзгерту-жоюды құру, автоматтандырылған жүйелерді (АЖ) пайдаланушылардың есептік жазбаларына өзгерістер енгізу процесі, пошта жәшіктері мен электрондық пошта мекенжайларын құру, жою, атауларын өзгерту, пошта жіберілімінің қауіпсіздік топтары мен топтарын құру, жою, өзгерту, сондай-ақ АЖ пайдаланушыға қолжетімді ақпараттың не ресурстардың көлемін кеңейтуге (қысқартуға) алып келетін басқа да өзгерістер.

2. Ереженің мақсаты мен қолданылу

саласы

2.1. Ереже колледжде ақпараттық қауіпсіздікті қамтамасыз етуді ұйымдастыру тәртібі мен ережелерін, колледж бөлімшелері мен қызметкерлері арасында ақпараттық қауіпсіздікті қамтамасыз ету функциялары мен жауапкершілігін бөлуді, колледжде қолданылатын ақпараттық құралдарға ақпараттық қауіпсіздік бойынша талаптарды регламенттейді.

2.2. Ереже колледждің жергілікті нормативтік актісі болып табылады. Осы Ереженің талаптары колледждің барлық құрылымдық бөлімшелері үшін міндетті және:

автоматтандырылған колледж жүйелері;

телекоммуникация құралдары;

Үй-жайлар;

колледж қызметкерлері.

2.3. Ереже белгіленген тәртіппен колледж директорының бұйрығымен бекітіледі.

3. Жалпы ережелер

3.1. Ақпараттық қауіпсіздік колледждің кешенді қауіпсіздігінің құрамдас элементтерінің бірі болып табылады. Колледждің ақпараттық қауіпсіздігі деп ақпараттық ресурстардың, оларды қалыптастыру және пайдалану технологияларының, сондай-ақ ақпараттық қызмет субъектілерінің құқықтарының қорғалу жағдайы түсініледі.

3.2. Ақпараттық қауіпсіздік-кешенді, криптографиялық, компьютерлік, ұйымдастырушылық, техникалық қорғау құралдарын қоса алғанда, ақпарат объектісінің, оның ішінде автоматтандырылған және телекоммуникациялық жүйелер объектілерінің қорғалған жай-күйін қамтамасыз етуге, техникалық барлауға қарсы іс-қимыл жасауға бағытталған қызмет.

3.3. Ақпараттық қауіпсіздікті қамтамасыз ету мынадай бағыттар бойынша жүзеге асырылады:

- құқықтық қорғау-ақпаратты құқықтық негізде қорғауды қамтамасыз ететін рәсімдер мен іс-шаралар;

- ұйымдастырушылық қорғау дегеніміз-орындаушылардың қызметі мен қарым-қатынасын нормативтік-құқықтық негізде реттеу, ол қандай да бір зиян келтіруді болдырмайды немесе әлсіретеді;

- инженерлік-техникалық қорғау-бұл зиян келтіруге кедергі келтіретін әртүрлі техникалық құралдарды пайдалану.

3.4. Ақпараттық қауіпсіздік мыналарды қамтиды:защиту интеллектуальной собственности колледжа;

- компьютерлерді, Жергілікті желілерді және интернет жүйесіне қосылу желісін қорғау;
- дербес деректерді қоса алғанда, құпия ақпаратты қорғауды ұйымдастыру; - қызметкерлер мен білім алушылар;
- құпия ақпараттың барлық жеткізгіштерін есепке алу;
- Колледждің ақпараттық қауіпсіздігін қамтамасыз ету керек:
- құпиялылық (ақпаратты рұқсатсыз ашудан қорғау немесе жол-жөнекей ұстап алу);
- тұтастық (ақпараттың және компьютерлік бағдарламалардың дәлдігі мен толықтығы);
- қолжетімділік (пайдаланушылардың өз құзыреті шегінде ақпарат алу мүмкіндігі).

3.5. Колледждің ақпараттық қауіпсіздік объектілеріне мыналар жатады:

- құпия сипаттағы мәліметтер тізбесіне сәйкес құжатталған ақпаратты қамтитын ақпараттық ресурстар;
- қорғалуы ҚР заңнамалық актілерінде көзделген ақпарат, оның ішінде дербес деректер де;
- қол жетімділігі шектеулі ақпаратты қабылдауды, өңдеуді, сақтауды және беруді жүзеге асыратын ақпараттандыру құралдары мен жүйелері, бағдарламалық құралдар, автоматтандырылған басқару жүйелері, байланыс және Деректер беру жүйелері.

3.6. Ереженің құқықтық негізін мыналар құрайды:

Қазақстан Республикасының Конституциясы (23.03.2019 жылғы жағдай бойынша өзгерістермен және толықтырулармен);

"Қазақстан Республикасының Ұлттық қауіпсіздігі туралы" заң (16.11.2020 жылғы жағдай бойынша өзгерістермен және толықтырулармен);

"Байланыс туралы" 2004 жылғы 5 шілдедегі № 567-ІІ Қазақстан Республикасының Заңы (02.07.2020 жылғы жағдай бойынша өзгерістермен және толықтырулармен);

"Ақпаратқа қол жеткізу туралы" Қазақстан Республикасының Заңы (28.12.2016 ж. жағдай бойынша өзгерістермен және толықтырулармен)

"Дербес деректер және оларды қорғау туралы" Қазақстан Республикасының Заңы (12.03.2021 жылғы жағдай бойынша өзгерістермен және толықтырулармен);

Қазақстан Республикасының ақпараттық қауіпсіздікті қамтамасыз ету саласындағы басқа да заңнамалық актілері, басшылық және нормативтік-әдістемелік құжаттары.

4. Ақпарат қауіпсіздігін қамтамасыз етудің мақсаттары мен міндеттері

Колледжде айналатын ақпараттың қауіпсіздігін қамтамасыз етудің басты мақсаты Қазақстан Республикасының заңнамалық актілерінің ережелерін және

қолжетімділігі шектеулі ақпаратты (бұдан әрі мәтін бойынша – құпия немесе қорғалатын ақпарат) қорғау бойынша нормативтік талаптарды іске асыру және ақпаратты жария ету, жоғалту, жылыстату, бұрмалау және жою, оны заңсыз пайдалану және колледждің ақпараттық-телекоммуникациялық жүйесінің жұмысын бұзу нәтижесінде залалдың алдын алу болып табылады.

Ақпарат қауіпсіздігін қамтамасыз етудің негізгі мақсаттары:

кетуінің алдын алу, ұрланудан, бұрмаланудан, жалған ақпарат жасаудан ақпарат, циркуляциялық колледжде;

білім алушылардың, колледж қызметкерлерінің ақпараттың құпиялылығын сақтауға жеке құқықтарының бұзылуын болдырмау;

ақпаратты брондау бойынша рұқсат етілмеген әрекеттердің алдын алу.

4.3. Ақпарат қауіпсіздігін қамтамасыз етудің негізгі міндеттері:

заңнамалық актілердің ережелеріне және ақпаратты қорғау жөніндегі нормативтік талаптарға сәйкестігі;

ақпараттық қауіпсіздік қатерлерінің көздерін, колледж мүдделеріне зиян келтіруге, колледждің қалыпты жұмыс істеуі мен дамуына ықпал ететін себептер мен жағдайларды уақтылы анықтау, бағалау және болжау;

ақпараттық қауіпсіздік қатерлеріне және ақпараттық қатынастар жүйесіндегі теріс үрдістерге жедел ден қою тетігін құру;

техникалық құралдар мен ақпараттық технологияларға, оның ішінде ұйымдық-құқықтық және техникалық шаралар мен ақпаратты қорғау құралдарын пайдалана отырып, ақпараттық ресурстарға заңсыз қол сұғудың тиімді жолын кесу;

ақпаратты қорғауды қамтамасыз ету бойынша колледждің құрылымдық бөлімшелерінің қызметін үйлестіру;

қорғау жүйесін дамыту, оны ұйымдастыруды, оның нысандарын, әдістерін және ақпараттық қауіпсіздік қатерлерін болдырмау, парилірлеу және бейтараптандыру және оны бұзу салдарларын жою құралдарын жетілдіру;

қорғалған заңдық маңызы бар электрондық құжат айналымын дамыту және жетілдіру;

ақпараттық қауіпсіздік жүйесін бақылауды қамтамасыз ететін тетіктерді құру және ақпараттық қауіпсіздіктің белгіленген талаптарын орындаудың сенімділігіне кепілдік беру;

ақпараттық қауіпсіздік жүйесін (ИБЖ) басқару тетіктерін құру.

5. Ақпараттық қауіпсіздікті қамтамасыз ету жүйесін ұйымдастыру

5.1. Ақпараттық қауіпсіздікті қамтамасыз ету жүйесінің алдында тұрған міндеттерді іске асыру мақсатында колледжде:

- қызметкерлер мен білім алушылардың дербес деректерін қорғау;
- колледж қызметін ақпараттық қамтамасыз етудің электрондық құралдарының тікелей мақсаты бойынша пайдаланылуын бақылау;
- ақпараттың орын ауыстыруын желішілік бақылау;

- қолданыстағы заңнамаға сәйкес экстремистік деп танылған ақпараттық материалдарға қол жеткізуге тыйым салу шараларын қабылдау;
- колледж персоналы мен білім алушыларының оларға әкімшілік беретін Интернет-ресурсты пайдалануының орындылығын тексеру, жол берілетін бұзушылықтарды талдау және оны техникалық қарсы іс-қимыл құралдарымен мақсатсыз пайдалануына жол бермеу шараларын қабылдау;
- персонал мен білім алушылардың дербес деректерін қорғау-автоматтандыру құралдарын пайдалана отырып немесе осындай құралдарды пайдаланбай, оларды өңдеу кезінде персонал мен колледж білім алушыларының дербес деректеріне рұқсатсыз қол жеткізуге жол бермеу жөніндегі іс-шаралар;
- колледждің құрылымдық бөлімшелері бойынша колледж қызметін ақпараттық қамтамасыз етудің электрондық құралдарының пайдаланылуына бақылау жасау (директордың АТ жөніндегі орынбасары, директордың ОІ жөніндегі орынбасары, директордың ОІЖ жөніндегі орынбасары, директордың ОІЖ жөніндегі орынбасары, директордың ОІЖ жөніндегі орынбасары, бөлім меңгерушілері, колледж кітапханасы, кадрлар бөлімі);
- қолданыстағы заңнамаға сәйкес экстремистік деп танылған ақпараттық материалдарға қол жеткізуге тыйым салу шараларын қабылдау, бұл мәліметтерді колледж әкімшілігі мен персоналына жеткізу және осы материалдарға қол жеткізуге тыйым салу шараларын қабылдау (интернет желісіндегі материалдарға қатысты – техникалық қарсы іс-қимыл шараларымен);

колледж персоналы мен білім алушыларының оларға әкімшілік беретін интернет – ресурсты пайдалануының орындылығын тексеру, жол берілетін бұзушылықтарды талдау және оны техникалық қарсы іс-қимыл құралдарымен мақсатсыз пайдалануына жол бермеу шараларын қабылдау колледж әкімшілігі беретін ресурсты пайдалану кезінде шектеулер туралы жалпыға бірдей қолжетімді талаптарды колледж персоналы мен білім алушыларына Нұсқаулық нысанында белгілеу және жеткізу, көрсетілген шектеулердің орындалуын тұрақты бақылау, туындаған бұзушылықтарға не теріс пайдалануларға қарсы іс-қимылдың техникалық (бағдарламалық) құралдарын әзірлеу, енгізу және қолдану;

ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша колледж персоналын оқыту:

колледждің ақпараттық қауіпсіздігін қамтамасыз ету бойынша талаптарды сақтауға мүмкіндік беретін тиісті білімді, іскерлікті және дағдыларды қалыптастыру мақсатында персоналмен сабақтар өткізу.

5.2. Колледждің ақпараттық қауіпсіздік жүйесіне жалпы басшылықты директордың ақпараттық технологиялар жөніндегі орынбасары жүзеге асырады. Колледждің құрылымдық бөлімшелерінің басшылары оны тиісті жағдайда ұстауға, өз қызметінің бағыттары бойынша одан әрі дамыту мен жетілдіруге қатысуға міндетті.

6. Парольдерге қойылатын талаптар

6.1. Құпиясөзді таңдау кезінде келесі ережелерді басшылыққа алу қажет:

парольдің ұзындығы кемінде 8 таңбадан тұруы керек;

парольді таңдағанда кіші және үлкен әріптердің, сандардың тіркесімін пайдалану ұсынылады;

құпия сөз ретінде тіркелгі атауын немесе пайдаланушы атын, сондай-ақ таңбалардың оңай табылған тіркесімін пайдалануға тыйым салынады.

Пайдаланушы құпиясөзді құпия сақтауға дербес жауапты болады. Парольді басқа тұлғаларға хабарлауға, оны жазуға, сондай-ақ электрондық хабарламаларда ашық мәтінмен жіберуге тыйым салынады.

Пайдаланушы осы Ереженің талаптарын сақтай отырып, кемінде үш айда бір рет парольді өзгертуге міндетті.

Пароль жария етілген жағдайда (немесе жария етуге күдікті болса) бұл туралы дереу БҚ маманына хабарлау және парольді өзгерту қажет.

Пайдаланушының ұмытылған паролін қалпына келтіруді БҚ жөніндегі маман Пайдаланушының жазбаша өтінімі негізінде пайдаланушының паролін өзгерту (қалпына келтіру) жолымен жүзеге асырады.

Пайдаланушының парольді өзгертуге ауызша өтінімі мұндай өзгерістерді жүргізу үшін негіз болып табылмайды.

Парольдердің алдын алу үшін бағдарламалық жасақтама маманы парольді үш рет қате енгізген кезде Есептік жазбаны құлыптау механизмін конфигурациялауға міндетті.

7. Интернет ресурстарына қол жеткізу

7.1. Өндірістік қызметпен байланысты міндеттерді орындау үшін колледж қызметкерлеріне интернет ресурстарына қолжетімділік беріледі. Интернет ресурстарына басқа мақсаттарда қол жеткізуге тыйым салынады.

7.2. Қол жеткізудің талап етілетін деңгейі колледж қызметкеріне Ақпараттық технологиялар жөніндегі директордың "қол жеткізу тізімдерін өзгертуге" өтінімі негізінде ұсынылады.

7.3. ПО маманы колледж басшысына алдағы айға Интернетті пайдалану лимитін ұсынуға міндетті.

7.4. БҚ жөніндегі маман айына кемінде бір рет колледж қызметкерлерінің ақпараттық технологиялар жөніндегі директорға интернет-ресурстарды пайдалануы туралы есеп беруге міндетті.

7.5. Интернет ресурстарына қолжетімділікті БҚ жөніндегі маман штаттан тыс жағдайлар туындаған кезде не ұйымдастырушылық құжаттарда көзделген өзге де жағдайларда алдын ала хабарламай бұғаттай алады.

7.6. Колледж қызметкерлеріне колледж директорының атына жазылған өтінішке сәйкес қосымша Интернет-трафик берілуі мүмкін.

7.7. Интернет ресурстарымен жұмыс істеу қағидалары 1-қосымшада келтірілген.

8. Электрондық пошта

- 8.1. Өндірістік қызметке байланысты міндеттерді орындау үшін колледж қызметкерлеріне электрондық поштаға рұқсат берілуі мүмкін. Колледждің электрондық поштасын басқа мақсаттарда пайдалануға тыйым салынады.
- 8.2. Электрондық поштаға қол жеткізу колледж қызметкеріне "қол жеткізу тізімдерін өзгерту" өтінімі негізінде беріледі.
- 8.3. Электрондық пошта колледждің меншігі болып табылады және оны тек қызметтік мақсатта пайдалануға болады. Электрондық поштаны басқа мақсаттарда пайдалануға қатаң тыйым салынады.
- 8.4. Қызметкердің электрондық пошта жәшігінің ішіндегісі басшылықтың талабы бойынша алдын ала ескертусіз тексерілуі мүмкін.
- 8.5. Электрондық поштаның жұмысын қамтамасыз ету құралдарының жұмыс параметрлерінде елеулі ауытқулар анықталған жағдайда, бағдарламалық қамтамасыз ету жөніндегі маман шешім қабылдау үшін бұл туралы ақпараттық технологиялар жөніндегі директорға дереу хабарлауға міндетті.
- 8.6. Электрондық поштаға қолжетімділікті БҚ жөніндегі маман штаттан тыс жағдайлар туындаған кезде не Ұйымдастыру құжаттарында көзделген өзге де жағдайларда алдын ала хабарламай бұғаттауы мүмкін.
- 8.7. Электрондық поштамен жұмыс істеу қағидалары 3-қосымшада келтірілген.

9. Вирусқа қарсы қорғаныс

- 9.1. Колледжде пайдалануға аталған құралдарды әзірлеушілерден (жеткізушілерден) орталықтандырылып сатып алынған лицензиялық вирусқа қарсы құралдар ғана рұқсат етіледі.
- 9.2. Колледждің компьютерлерінде (ЛВС серверлерінде) вирусқа қарсы бақылау құралдарын орнатуды уәкілетті қызметкерлер жүзеге асырады.
- 9.3. Вирусқа қарсы бақылау құралдарының параметрлерін баптауды нақты вирусқа қарсы құралдарды қолдану жөніндегі нұсқаулықтарға сәйкес БҚ жөніндегі маман жүзеге асырады. Басқа қызметкерлердің параметрлерін өзгертуге тыйым салынады.
- 9.4. Күн сайын жұмыстың басында компьютерді (ЛВС серверлері үшін – қайта іске қосу кезінде) автоматты режимде жүктеу кезінде барлық дискілер мен файлдарға вирусқа қарсы бақылау жүргізілуі тиіс.
- 9.5. Міндетті вирусқа қарсы бақылауға телекоммуникациялық арналар арқылы алынатын және берілетін кез келген ақпарат (кез келген форматтағы мәтіндік файлдар, деректер файлдары, орындалатын файлдар), сондай-ақ алмалы-салмалы жеткізгіштердегі (магниттік дискілердегі, CD-ROM және т.б.) ақпарат жатады.
- 9.6. Вирусқа қарсы тексеру жүргізілуі тиіс:
 - қызметкерлердің компьютерлерінде-аптасына кемінде бір рет; – ЛВС серверлерінде-аптасына кемінде екі рет.

9.7. Компьютерлік вирустың болуына күдік туындаған кезде (бағдарламалардың атиптік жұмысы, графикалық және дыбыстық әсерлердің пайда болуы, деректердің бұрмалануы, файлдардың жоғалуы, жүйелік қателер туралы хабарламалардың жиі пайда болуы және т.б.) бөлімше қызметкері БҚ жөніндегі маманмен бірлесіп өзінің ДҚ-не кезектен тыс вирусқа қарсы бақылау жүргізуі тиіс.

10. Деректерді сақтау

10.1. Колледж қызметкерлерінің қызметтік ақпараты колледждің ЛВС серверлерінде арнайы бөлінген папкаларда сақталуы тиіс. Қызметкерлердің компьютерлерінде қызметтік ақпаратты сақтауға тыйым салынады.

10.2. Жауапкершілік:

10.2.1. Колледж серверлерінде сақталатын деректердің тұтастығын қамтамасыз ету үшін жауапкершілік осы Ереженің талаптарына сәйкес БҚ жөніндегі маманға жүктеледі.

10.2.2. Колледж қызметкерлерінің жергілікті компьютерлерінде сақталатын деректердің тұтастығын қамтамасыз ету үшін жауапкершілік осы Ереженің талаптарына сәйкес қызметкерлердің өздеріне жүктеледі.

11. Жабдықтарды орнату және қызмет көрсету

11.1. Жабдықты орнату және қызмет көрсету тек бағдарламалық жасақтама маманымен мүмкін. Басқа қызметкерлердің жабдықты орнатуына және қызмет көрсетуіне тыйым салынады.

11.2. Жабдықты рұқсатсыз ауыстыруды анықтау үшін колледждің барлық техникасы ашылуы мүмкін жерлерде мөрленуі керек.

11.3. Жабдықтың жұмысындағы іркілістер үшін жауапкершілік БҚ жөніндегі маманға жүктеледі.

12. Бағдарламаларды орнату және қызмет көрсету

12.1. Бағдарламаларды орнату тек бағдарламалық жасақтама маманымен мүмкін. Басқа қызметкерлерге бағдарламаларды орнатуға тыйым салынады.

Ереже

колледж қызметкерлері мен білім алушылардың компьютерлік желілердегі жұмыстары

Осы Қағидалар колледждің компьютерлік желісінде және Интернет желісінде (бұдан әрі-желі) жұмыс істеуге байланысты білім алушылардың құқықтары мен міндеттерін, сондай-ақ жұмыстың негізгі қағидаларын және колледж оқытушылары мен қызметкерлерінің өкілеттіктерін реттейді. Ережелер студенттердің қауіпсіздігі мен қауіпсіздігін қамтамасыз ету жөніндегі шаралар жүйесімен бірге желілердің білім беру әлеуетін пайдалануды қамтамасыз етуге және ұйымдастыруға арналған.

Желілерде жұмыс істеу үшін колледж саясатының негізгі принциптері:

барлық білім алушылар үшін тең қолжетімділік;

білім алушылардың желілерді тек білім беру мақсаттары үшін пайдалануы;

оқушыларды зорлық-зомбылық пен терроризмді, этникалық және діни төзбеушілікті, есірткіні, құмар ойындарды және т.б. насихаттауды қамтитын зиянды немесе заңсыз ақпараттан қорғау.

Оқытушылар мен қызметкерлердің өкілеттіктері:

осы ережені іске асыру бойынша барлық қызметті ұйымдастырады және басқарады;

колледждің оқу бағдарламасына және мүмкіндіктеріне сәйкес білім алушылардың желілерге еркін және тең қолжетімділігін қамтамасыз етеді;

осы Ережені іске асыру бойынша барлық қызметті ұйымдастырады және басқарады;

желілер арқылы білім беру процесін байыту және кеңейту үшін мүмкіндіктер жасайды;

қолданыстағы заңнамаға сәйкес білім алушылардың желілердегі зиянды немесе заңсыз мазмұн ресурстарына қол жеткізуін шектеу бойынша провайдермен ынтымақтастықты қоса алғанда, шараларды ұйымдастыруға жауап береді;

оқу бөлімінде білім алушылар топтары үшін Интернет желісіне қолжетімділік ашуға оқытушылардың өтінімдерінің күнтізбелік-тақырыптық жоспарға сәйкестігін тексереді. Бұл топ үшін сабаққа қажетті сайттар тізімі бойынша сабақ уақытында кіруге мүмкіндік береді;

білім алушылардың желілерде жұмыс істеу ережелерінің сақталуын бақылауды қамтамасыз етеді;

колледж желісі арқылы Берілетін трафик мониторингі саласында техникалық мүмкіндіктер береді;

әр оқу жылының басында білім алушыларды желідегі қауіпсіз жұмыс ережелерімен таныстыруды ұйымдастырады, білім алушыларға трафиктің бақыланатынын хабарлайды;

сайтты қолдауды және жаңартуды ұйымдастырады, сайтқа директор бекіткен материалдарды ғана орналастырады;

бұзушылықтардың анықталғаны туралы директорға дереу хабарлайды және бұзушылықтарды жою жөнінде шаралар қабылдайды.

- білім беру қызметін байыту және кеңейту мақсатында интернет мүмкіндіктерін пайдалану, ол үшін білім алушыларға нақты тапсырмалар тағайындау және тиісті интернет-мекенжайлардың тізбесін келтіру;
- күнтізбелік-тақырыптық жоспарларда көзделген оқу сабақтары шегінде білім алушылар тобына рұқсат беруге, сондай-ақ негіздемемен қажетті ресурстар тізбесін көрсете отырып, оқу жоспарларынан тыс қол жеткізуді ашу үшін өтінімдерді уақтылы беруге; оқу уақытында желілерде білім алушылардың жұмысын үздіксіз бақылауды жүзеге асыру;
- білім алушылардың желілердегі тыйым салынған мазмұн ресурстарына қол жеткізуін тоқтату үшін шұғыл шаралар қабылдау;
- ережелерді бұзу туралы немесе колледж желісінде заңсыз контент құру туралы дереу маманға хабарлаңыз;
- оқу сабақтары кезінде оқу кабинетінен шықпауға және желідегі жұмысқа үзіліс кезінде білім алушыларды жібермеуге;
- Оқытушылар сабақтар өткізілетін оқу кабинетіне бекітілген колледж жабдықтарының тұтастығына жауап береді.

Білім алушылардың құқықтары мен міндеттері:

- тең қол жеткізу желілеріне саясатын ескере отырып, колледждің ақпараттандыру; - Интернет желісіне қол жеткізу (тек оқытушының бақылауымен);
- желілердегі жұмыс ережелері туралы хабардар болыңыз.

Білім алушылар келесі ережелерді сақтауға міндетті:

- осы сабақ үшін оқытушыларға тізбеге енгізілмеген сайттарға шығуға тыйым салынады;
- зорлық-зомбылық пен терроризмді, этникалық және діни төзбеушілікті, есірткіні, құмар ойындарды және т. б. насихаттайтын материалдарды анықтаған кезде мұғалімге дереу хабарлаңыз.;
- желілерді тек білім беру мақсаттары үшін пайдалану;
- қорлайтын, қорқытатын немесе әдепсіз хабарламаларды жібермеуге немесе оларға жауап бермеуге тиіс; колледждің компьютерлік желісінің тұтастығына қауіп төндіретін немесе басқа жүйелерге шабуыл жасайтын кез келген қызметті жүргізуге тыйым салынады;
- біреудің пайдаланушы аты, құпия сөзі және электрондық поштасын пайдалануға тыйым салынады;
- лицензияланбаған бағдарламалық жасақтаманы, авторлық құқықпен қорғалған материалдарды рұқсатсыз және авторлық құқықты бұзатын кез-келген басқа қызметті пайдалануға тыйым салынады.

Жауапкершілік

Білім алушылар осы Қағидалардың ережелерін бұзғаны үшін Колледждің ішкі тәртіп қағидаларына сәйкес тәртіптік жауапкершілікке тартылады.

Оқытушылар мен қызметкерлер осы Қағидалардың ережелерін бұзғаны үшін Қазақстан Республикасының Еңбек кодексіне сәйкес жауапты болады және тәртіптік жауапкершілікке тартылады.

Қылмыс, әкімшілік құқық бұзушылық болып табылатын немесе меншікке зиян келтіретін бұзушылықтар үшін кінәлілер Қазақстан Республикасының заңнамасына сәйкес жауапты болады.

Қосымша 2

Интернет ресурстарымен жұмыс істеу ережелері

Ғаламдық Интернет әртүрлі мазмұндағы және бағыттағы ресурстарға қол жетімділікті қамтамасыз етеді. Колледж бойынша маман мазмұны қызметтік міндеттерін орындауға қатысы жоқ Интернет желісінің ресурстарына, сондай-ақ мазмұны мен бағыты Халықаралық және қазақстандық заңнамамен тыйым салынған ресурстарға, оның ішінде зиянды, қауіп төндіретін, жала жабатын, әдепсіз ақпарат, сондай-ақ басқа тұлғалардың ар-намысы мен абыройын қорлайтын материалдарға, ұлттық алауыздықты қоздыратын, зорлық-зомбылықты туғызатын, құқыққа қарсы әрекет жасауға шақыратын материалдарға қол жеткізуді шектеуге құқылы., оның ішінде жарылғыш заттар мен өзге де қаруды қолдану тәртібін түсіндіретін және т. б. Интернет ресурстарымен жұмыс істеу кезінде жол берілмейді:

- қызметтік қажеттілік бойынша немесе өзге жолмен колледж қызметкеріне белгілі болған колледждің коммерциялық және қызметтік ақпаратын жария ету;
- қандай да бір патентке, сауда маркасына, коммерциялық құпияға, копирайтқа немесе өзге де меншік құқықтарына және/немесе үшінші тараптың авторлық және онымен сабақтас құқықтарына қатысты авторлық құқықтармен қорғалатын материалдарды тарату;
- вирустары немесе басқа да компьютерлік кодтары, файлдары немесе бағдарламалары бар, кез келген компьютерлік немесе телекоммуникациялық жабдықтың немесе бағдарламалардың функционалдығын бұзуға, жоюға не шектеуге арналған материалдарды, сондай-ақ коммерциялық бағдарламалық өнімдерге сериялық нөмірлерді және оларды генерациялауға арналған бағдарламаларды, интернеттегі ақылы ресурстарға рұқсатсыз қол жеткізуге арналған логиндерді, парольдерді және өзге де құралдарды жариялау, жүктеу және тарату, сондай-ақ жоғарыда көрсетілген ақпаратқа сілтемелерді орналастыру.
- Интернет ресурстарымен жұмыс істеу кезінде тыйым салынады: вирусқа қарсы пакетте орнатылған вирустардың болуын алдын ала тексермей орындалатын немесе өзге де файлдарды жүктеу және іске қосу;

- колледж саясатымен пайдалануға тыйым салынған ресурсқа қол жеткізуге мүмкіндік беретін бағдарламалық және аппараттық құралдарды пайдалану.

- Ресурсқа кіру мүмкіндігі сұралған ресурстың рұқсат етілген колледж саясаты екендігінің кепілі емес.

- Колледж қызметкерлері кіретін ресурстар туралы барлық ақпарат тіркеледі және қажет болған жағдайда бөлім басшыларына, сондай-ақ колледж әкімшілігіне егжей-тегжейлі зерттеу үшін ұсынылуы мүмкін.

Қосымша 3

Ереже электрондық пошта

Электрондық пошта колледждің меншігі болып табылады және оны тек қызметтік мақсатта пайдалануға болады. Электрондық поштаны басқа мақсаттарда пайдалануға қатаң тыйым салынады.

Қызметкердің электрондық пошта жәшігінің ішіндегісі тікелей не жоғары тұрған басшының талап етуі бойынша алдын ала хабардар етпестен тексерілуі мүмкін.

- Электрондық поштамен жұмыс істеу кезінде колледж қызметкерлеріне тыйым салынады: пошта мекенжайын жазылымдар мен жаппай жіберілімдерді ресімдеу үшін пайдалану;

- өз мекенжайыңызды немесе колледждің басқа қызметкерлерінің мекенжайларын жалпыға қолжетімді Интернет ресурстарда (форумдар, конференциялар және т. б.) жариялау;

- кіріс хабарламалардағы кірістірілген файлдарды антивирустық құралдармен алдын-ала тексерусіз ашыңыз, тіпті хат жіберуші жақсы белгілі болса да;

- пошта хабарламаларын (10-нан астам) сыртқы адресаттарға олардың келісімінсіз жаппай таратуды жүзеге асыру. Бұл әрекеттер СПАМ ретінде анықталады және заңсыз болып табылады;

- жарнамалық сипаттағы пошта хабарламаларын жаппай таратуды жүзеге асыру;

- электрондық пошта арқылы құрамында вирустар немесе басқа да компьютерлік кодтар, файлдар немесе бағдарламалар бар, кез келген компьютерлік немесе телекоммуникациялық жабдықтың немесе Бағдарламаның функционалдығын бұзуға, жоюға немесе шектеуге арналған материалдарды, сондай-ақ коммерциялық бағдарламалық өнімдерге сериялық нөмірлерді және оларды генерациялауға арналған бағдарламаларды, интернеттегі ақылы ресурстарға рұқсатсыз қол жеткізуге арналған логиндерді, парольдерді және өзге де құралдарды, сондай-ақ жоғарыда көрсетілген ақпаратқа сілтемелерді тарату; қандай да бір патентке, сауда маркасына, коммерциялық құпияға, копирайтқа немесе өзге де меншік құқықтарына және/немесе үшінші

тараптардың авторлық және онымен сабақтас құқықтарына қатысты авторлық құқықтармен қорғалатын материалдарды тарату;

мазмұны мен бағыттылығы халықаралық және қазақстандық заңнамамен тыйым салынған ақпаратты, оның ішінде зиянды, қауіп төндіретін, жала жабатын, әдепсіз ақпарат, сондай-ақ басқа тұлғалардың ар-намысы мен абыройын қорлайтын материалдарды, ұлттық алауыздықты қоздыратын, зорлық-зомбылық жасауға итермелейтін, құқыққа қарсы әрекет жасауға шақыратын, соның ішінде жарылғыш заттар мен өзге де қаруды қолдану тәртібін түсіндіретін және т. б. материалдарды қоса таратуға, коммерциялық құпия болып табылатын қолжетімділігі шектеулі ақпаратты;

пошта мекенжайына кіру үшін кез-келген адамға құпия сөз беріңіз.

**Орындаушылар: Кубжасарова Ж. И.,
директордың АТ жөніндегі орынбасары,
Кушаев, М АТ бойынша маман**