

Каралды
Педагогикалык кеңештин
№ 1 протоколунда
«29» август 2022 жыл

Бекитем

94 жалпы орто билим берүү
мектебинин директорунун
милдетин аткаруучу
Ажыгулова К.К.



Билим берүү бөлүмүнүн маалыматтык системасы жөнүндө (ИСУО)

ЖОБО.

1. Жалпы жоболор.

1.1. Бул Регламент Кыргыз Республикасынын Өкмөтүнүн 2019-жылдын 17-июлундагы № 295 “Жалпы билим берүү уюмдарында билим берүү чөйрөсүнүн коопсуздугун жогорулатуу боюнча Кыргыз Республикасынын Өкмөтүнүн айрым чечимдерине өзгөртүүлөрдү киргизүү тууралуу” токтомуна ылайык иштелип чыккан. Жалпы билим берүү уюмдары жөнүндө тыштуу жобонун 7, 14-1 пункттарына ылайык (КР Өкмөтүнүн 2013-жылдын 2-октябрындагы № 544, 2014-жылдын 17-сентябрындагы № 535, 17-ноябрь токтомдорунун редакцияларына ылайык, 2019-ж. Ка 295), 2019-жылдын 8-октябрындагы № 1245 Кыргыз Республикасында билим берүүнү башкаруунун маалыматтык системасын түзүү Концепциясы менен (1.1.4

1.2. Жобо директордун буйругу менен бекитилген баштапкы кесиптик бирлик билим берүү уюмунун профсоюздук комитетинин корутундусун эске алуу менен билим берүү уюмунун педагогикалык кеңешинин (мындан ары - ОК) чечими менен кабыл алынат. Бул Жобого өзгөртүүлөр жана толуктоолор баштапкы кесиптик бирлик уюмунун профсоюздук комитетинин корутундусун эске алуу менен ОК педагогикалык кеңештин чечими менен киргизилет.

1.3. Жобо жеке маалыматтардын маалымат системасынын персоналына карата талаптарды, кызматкерлердин жоопкерчилигинин даражасын, структурасын жана коопсуздуктун талап кылынган деңгээлин аныктайт.

1.4. Бул Регламенттин максаты: ОК коргоо объектилеринин коопсуздугун тышкы жана ички, атайылап жана атайылап эмес коркунучтардын бардык түрлөрүнөн камсыз кылуу, жеке маалыматтардын коопсуздугуна коркунучтарды (УБД) мүмкүн ишке ашыруудан келтирилген зыянды минималдаштыруу бөлүм саналат.

1.5. Жеке маалыматтардын коопсуздугу жеке маалыматтарды жок кылууга, өзгөртүүгө, блоктоого, көчүрүүгө, жайылтууга, ошондой эле башка уруксатсыз аракеттерге алып келиши мүмкүн болгон жеке маалыматтарга уруксатсыз, анын ичинде докусунай кирүүнү болтурбоо аркылуу жетишилет.

1.6. Бул Жобонун колдонуу мөөнөтү чектелбейт. Жобо жаңысы кабыл алынганга чейин күчүндө болот.

2. Колдонуу чөйрөсү.

2.1. Билим берүүнү башкаруунун маалыматтык системасы (БМИС) - билим берүү системасынын жетекчилеринин, билим берүү тутумунун кызматкерлеринин маалыматтык керектөөлөрүн канааттандыруу үчүн маалыматты чогултууну, иштеп чыгууну, сактоону жана жайылтууну камсыз кылуучу эсеппөөчү жана байланыш техникасын, программалык камсыздоону, маалымат массивдерин, колдонуучуларды, процедураларды камтыган комплекс жана башка кызыкдаг тараптар. Билим берүүнү башкаруунун маалыматтык системасы билим берүү системасында маалыматты чогултуу, сактоо, жайылтуу, ошондой эле бардык деңгээлдеги билим берүүнү башкаруу органдарынын башкаруу ишин автоматташтыруу үчүн иштелип чыккан.

2.2. ИСУО түзүү төмөнкү принциптерге негизделген:

- баштапкы маалыматты бир жолу киргизүү жана көп жолу колдонуу, анын ичинде билим берүүнү башкаруу максаттары үчүн;
- структуралык дизайнды колдонуу. ЭМИС салыштырмалуу көз карандысыз функционалдык подсистемалардан турушу керек;
- классификациялоонун жана коддоонун бирдиктүү тутумун колдонуу аркылуу билим берүү органдарынын маалыматтык системаларынын пайкоштигин камсыз кылуу;
- жеке маалыматтарды, статистикалык маалыматтарды жана электрондук документ алмашууну ведомстволор аралык биргелешип пайдалануу бөлүгүндө билим берүү маалымат системаларын бири-бири менен жана башка бөлүмдөрдүн маалыматтык ресурстары менен интеграциялоо мүмкүнчүлүгү;
- Кыргыз Республикасынын мыйзамдарынын талаптарына ылайык маалыматтык коопсуздугу жана жеке маалыматтарды коргоо системасын камсыз кылуу;
- ИСУОну иштеп чыгууну, киргизүүнү жана колдоону борборлоштурулган башкаруу;
- ИСУО подсистемаларын негизинен интернет аркылуу иштөө мүмкүнчүлүгү бар веб-тиркемелер түрүндө түзүү;

колдонуудагы программалык-аппараттык каражаттардын максималдуу сакталышын эске алуу менен жаңы ЭМБС компоненттерин модернизациялоо жана өнүктүрүү жөнүндө чечим кабыл алуу;

ИСУОнун кеңейтилиши/масштабынын камсыз кылуу - жаңы функцияларды кошуу же иштеп жаткандардын айрымдарын ИСУОнун калган функциялардын бөлүктөрүн өзгөртүүсүз өзгөртүү мүмкүнчүлүгү;

колдонуучунун атайын компьютердик окуусун талап кылбаган колдонуучуга ыңгайлуу ИСУО интерфейсин түзүү;

толук маалымдама колдонмосу менен ИСУО функционалдуулугун тейлөө;

үзгүлтүксүз өнүгүү принциби. ЭМБС дайыма өзгөртүлүп турууну шарттардын - мыйзамдардагы, билим берүү системасынын түзүмүндөгү, маалыматтык технологиялардагы жана башкалардын өзгөрүшүнө байланыштуу өзгөртүүлөрдү киргизүүнүн мүмкүн болуучу зарылдыгын эске алуу менен түзүлөт.

2.3. ИСУОнун негизги функциялары жана функционалдык блоктору:

Кыргыз Республикасынын билим берүү системасында электрондук документ жүгүртүү жана өз ара аракеттенүү системасы төмөнкүлөрдү камсыз кылууга тийиш:

документтин кыймылы жөнүндө маалыматты сактоо жана документтин колдонулушунун ар бир көл-өрмөсүндө документтин же бул документтин өзүнчө талпырмасынын аткарылышы үчүн жооптуу адамды аныктоо мүмкүнчүлүгү;

документтердин кайталануу мүмкүнчүлүгүн жокко чыгарууга мүмкүндүк берүүчү документтик маалыматтын маалымат базасын сактоо;

документ файлдарын сактоо;

маалыматтарды көрүү жана көргөз, ошондой эле документалдык маалыматтарга жана документтерге кирүү укуктарын чектөө системасы;

идентификация - жеткиликтүүлүктүн субъектерине жана объектерине идентификаторду ыйгаруу жана же берилген идентификаторду ыйгарылган идентификаторлордун визмеси менен салыштыруу;

ИСУО - маалыматтар базасында камтылган жеке маалыматтардын, ошондой эле мындай жеке маалыматтарды автоматташтыруу каражаттарын пайдалануу менен же мындай каражаттарды колдонбостон иштетүүгө мүмкүндүк берүүчү маалыматтык технологиялардын жана техникалык каражаттардын жыйындысы болуп саналган маалыматтык система;

□ маалыматтык технологиялар - процесстер, издөөнүн, чогултуунун, сактоонун, иштеп чыгуунун, берүүнүн, таратуунун ыкмалары жана ушундай процесстерди жана ыкмаларды ишке ашыруу ыкмалары;

□ жеке маалыматтарды пайдалануу - жеке маалыматтардын субъектине же башка жактарга карата юридикалык кесепеттерге алып келүүнү же башка жактардын укуктарын жана эркиндиктерин таасир этүүчү чечимдерди кабыл алуу же башка аракеттерди жасоо максатында оператор тарабынан жеке маалыматтар менен жасалган аракеттер (операциялар), жеке маалыматтардын субъекти же башка адамдар;

□ маалыматтык коопсуздукка коркунуштун булагы - маалыматтык коопсуздукка коркунуч келтирген жетүү субъекти, материалдык объект же физикалык кубулуш;

□ жеке маалыматтардын купуялуулугу - жеке маалыматтардын субъектинин макулдугусуз же башка мыйзамдуу негиздерин алардын таркатылышына жол бербөө боюнча жеке маалыматтарга жетүү мүмкүнчүлүгүнө ээ болгон оператор же башка жак үчүн милдеттүү талап;

□ маалымат алып жүрүүчү - индивидуалдык же материалдык объект, анын ичинде маалымат символдор, сүрөттөр, сипаттар, техникалык чечимдер жана процесстер, физикалык чоңдуктардын сандык мүнөздөмөлөрү түрүндө чагылдырылган физикалык талап;

□ жеке маалыматтар (ИД) - анын фамилиясын, атын, атасынын, атын, жылы, айы, туулган күнү жана жери, дареги, дареге, дареге, анын ичинде аныкталган же ушундай маалыматтардын негизинде аныкталган жеке адамга тиешелүү ар кандай маалымат (жеке маалыматтардын предмети); үй-бүлө, социалдык, мүлктүк абалы, билими, кесиби, кирешеси, башка маалыматтар;

□ жеке маалыматтарды иштетүү - жеке маалыматтарды чогултуу, системалаштыруу, топтоо, сактоо, тактоо (жаңыртуу, өзгөртүү), пайдалануу, бөлүштүрүү (анын ичинде өткөрүп берүү), менчиктештирүү, бөгөттөө, жок кылуу же камтыган жеке маалыматтар менен аракеттер (операциялар);

□ жалпыга жеткиликтүү жеке маалыматтар - жетүү жеке маалыматтар субъектинин макулдугу менен чексиз сандагы адамдарга берилген же мыйзамдарга ылайык купуялуулуктун сакталыгы талап кылынбаган жеке маалыматтар;

□ же жеке маалыматтардын купуялуулугун кокусунан бузуу; жеке маалыматтарды

ачыкка чыгаруу - атайылап;

□ жеке маалыматтарды таратуу - жеке маалыматтарды адамдардын белгилүү бир чөйрөсүнө берүүгө (жеке маалыматтарды берүү) же чексиз сандагы адамдардын жеке маалыматтары менен таанышууга багытталган аракеттер, анын ичинде жеке маалыматтарды жалпыга маалымдоо каражаттарында ачыкка чыгаруу;

□ маалыматтык жана телекоммуникациялык тармактар же жеке маалыматтарга жетүү мүмкүнчүлүгүн ар кандай башка жол менен камсыз кылуу;

□ жеке маалыматтарды ментиктештирүү - натыйжада жеке маалыматтардын конкреттүү субъектисинин жеке маалыматтарга таандык экендигин аныктоо мүмкүн болбогон аракеттер;

□ жеке маалыматтарды жок кылуу - натыйжада жеке маалыматтардын маалымат системасында жеке маалыматтардын мазмунун калыбына келтирүү мүмкүн болбогон же анын натыйжасында жеке маалыматтардын материалдык алып жүрүүчүлөрү жок кылынган аракеттер;

□ техникалык каналдар аркылуу маалыматтын (корголгон) агын чыгышы - корголгон маалыматты алып жүрүүчүдөн маалыматты кармап турган техникалык каражатка физикалык чөйрө аркылуу маалыматты контролсуз таратуу;

□ аялуу - системаны же анда камтылган маалыматты бузуу үчүн колдонулушу мүмкүн болгон коргоо каражаттарынын аясыздыгы, маалыматтык бүтүздүгү - компьютердик техниканын же автоматташтырылган системанын кокустук жана/же атайылап бурмалоо (жок кылуу) шарттарында маалыматтын өзгөрбөсүгүн камсыз кылуу жөндөмдүүлүгү;

□ оператор (жеке маалыматтардын) - жеке маалыматтарды иштеп чыгууну уюштуруучу жана (же) күзөгө ашыруучу, ошондой эле жеке маалыматтарды иштетүүнүн максаттарын жана мазмунун аныктоочу мамлекеттик орган, муниципалдык орган, юридикалык же жеке жак;

□ жеке маалыматтардын маалыматтык системасынын техникалык каражаттары - компьютердик техника, маалыматтык-эсептөө системалары жана тармактары, жеке маалыматтарды берүү, кабыл алуу жана иштетүү үчүн каражаттар жана системалар (үн жазуу, үндү күчөтүү, үндү кайра чыгаруу каражаттары жана системалары, дөмофон жана телекөрсөтүү түзүлүштөрү); кеп, графикалык, видео жана алфавиттик-сандык маалыматтарды иштеп чыгуунун, документтерди жана башка

техникалык каражаттарды даярдоо каражаттары;

программалык камсыздоо (операциялык системалар, маалыматтар базасын башкаруу системалары ж.б.), маалыматтык системаларды колдонуучу маалыматты коргоо каражаттары.

3. Маалыматтык коопсуздуктун максаттары жана милдеттери.

3.1. Максаты: маалыматтык ресурстарга дурускасыз кирүүдөн коргоону камсыз кыла ал маалыматтык коопсуздук чараларын ишке ашыруу үб.

3.2. Маалыматтык коопсуздукту камсыз кылуунун негизги милдеттери болуп төмөнкүлөр болуп саналат:

• маалыматты санкцияланбаган кирүүдөн, жок кылуудан, өзгөртүүдөн, бөгөт коюудан, көчүрүүдөн, берүүдөн, тарагуудан, ошондой эле мындай маалыматка карата башка мыйзамсыз аракеттерден коргоону камсыз кылуу;

мүмкүнчүлүгү чектелген маалыматты сактоону уюштуруу;

маалыматка жетүү укугун ишке ашыруу;

маалыматты коргоонун техникалык жана программалык каражаттарын эксплуатациялоону уюштуруу.

Маалыматтык коопсуздуктун инструменттеринин жана системаларынын учурдагы иштөөсүн көзөмөлдөө,

маалыматтын резервдик көчүрмөсүн уюштуруу жана көзөмөлдөө.

4. Маалыматтык коопсуздукту камсыз кылуу үчүн жооптуу адамдар:

4.1. Маалыматтык коопсуздукту камсыз кылуу үчүн жооптуу адамдар (мындан ары - жооптуу адамдар) - жооптуу адамдар өздөрүнүн функционалдык милдеттеринин чегинде 1) Одогу маалыматтык каражаттарды колдонуу менен иштетилген, берилүүчү жана сакталган маалыматтык коопсуздуктун камсыз кылышат.

4.2. Маалыматтык коопсуздук кызматкерлери төмөнкү негизги функцияларды аткарышат:

маалыматтык коопсуздук боюнча нускамаларды иштен чыгуу: антивирустук коргоону уюштуруу боюнча инструменталар, Интернетте коопсуз серептөө боюнча нускамалар,

персоналдык компьютерлерди (мындан ары - ЖК) колдонуучуларды кызматкерлерди маалыматтык коопсуз иштетүү эрежелерине жана маалыматтык коопсуздук каражаттары менен иштөө эрежелерине окутуу;

- магниттик сактагычтарды жана CD/DVD келип түшкөн электрондук почта файлдарын антивирустук башкарууну уюштуруу.
 - иштеп жаткан программалык жана ашарагыч маалыматты коргоо каражаттарынын ден соолугуна жана натыйжалуулугуна учурдагы мониторинг.
 - ага уруксатсыз өзгөртүүлөрдү аныктоо үчүн ЖКда иштеген программалык камсыздоонун бүтүндүгүн көзөмөлдөө.
 - ыйгарым укуктуу программалык камсыздоону өзгөртүүнү, компьютерде алмаштырууну жана оңдоону көзөмөлдөө.
 - Интернетти колдонууну көзөмөлдөө.
5. Билим берүү уюмунун маалыматтык коопсуздугун камсыз кылуу боюнча жооптуу адамдардын милдеттери.
- 5.1. Өз милдеттеринин чегинде маалыматтык коопсуздук каражаттарынын жана системаларынын иштешин жана иштешин камсыз кылуу, ЖК кызматкерлеринин укук бузууларын жана санкцияланбаган аракеттерин аныктоо, бузууларды четтетүү боюнча зарыл чараларды көрүү.
- 5.2. ТООну тейлеген программисттер менен бирдикте (сүрдө келишим, макулдашуу ж.б.)
- 5.3. ЖК кызматкерлерине маалыматтык коопсуздук куралдары жана колдонулган системалар менен иштөө эрежелерин үйрөтүү.
- 5.4. Вируска каршы программалардын ишин көзөмөлдөнүз, жумасына бир жолу компьютерлерди вируска толук текшерүүдөн өткөрүңүз
- 5.5. Маалыматтарга уруксатсыз кирүүгө жана (же) анын маалыматка жетүү укугу жок адамдарга берилишине бөгөт коюу.
- 5.6. Маалыматтарга уруксатсыз жетүү фактыларын өз убагында аныктос.
- 5.7. Маалыматка жетүүнүн тартибин бузуунун жагымсыз кесепеттерин алдын алуу.
- 5.8. Маалыматты иштен чыгуунун техникалык каражаттарына таасир этүүнү болтурбоо. мунун натыйжасында алардын иштешин бузулат.
- 5.9. ТООдө маалыматтык коопсуздукту, жогорку деңгээлин камсыз кылууну дайыма көзөмөлдөө туруу.
6. Жеке маалыматтарды коргоону камсыз кылуу боюнча кызматкерлерге коюлуучу талаптар.
- 6.1. ИСУОнун колдонуучулары болуп саналган бардык ОО кызматкерлер корголуучу объектирге жетүү жана ПДнын кабыл алынган коопсуздук режимин сактоо боюнча

белгиленген эрежелерди жана милдеттерди так билүүгө жана так аткарууга тийиш.

6.2. АКБС Анын колдонуучулары болуп саналган бардык 00 кызматкерлер корголуучу объекттерге жетет жана ИДнын кабыл алган коопсуздук режимин сактоо боюнча белгиленген эрежелерди жана милдеттерди так билүүгө жана так аткарууга тийүү.

6.3. 00 кызматкерлери паролдорду тандоодо жана колдонууда (өгөр аутентификациянын техникалык каражаттары колдонулбаса) ИДнын коопсуздук режимин сактоонун белгиленген жол-жоболорун сактоого милдеттүү.

6.4. 00 кызматкерлери карбосуз калган жабдуулар үчүн тийиштүү коргоону камсыз кылууга

тийиш, айрыкча, уруксатсыз адамдар имаратка кире алган учурларда. Бардык колдонуучулар ИД коопсуздук талаптарын жана карбосуз калган жабдууларды коргоо жол-жоболорун, ошондой эле мындай коргоону камсыз кылуу боюнча өздөрүнүн милдеттерин билиши керек.

6.5. Кызматкерлерге үчүнчү тараптын программаларын орнотууга, жеке мобилдик гүзүлүштөрдү жана сактагычтарды туташтырууга, ошондой эле аларга коргоолтон маалыматты жазууга тыюу салынат.

6.6. Кызматкерлерге 00 маалыматтык системалар менен иштөөдө аларга белгилүү болгон коргоолтон маалыматты үчүнчү жактарга ачыкка чыгарууга тыюу салынат.

6.7. ИСУОдө ИД менен иштөөдө 00 кызматкерлери автоматташтырылган жумуш орунунун

мониторлорунан (AWP) үчүнчү жактар ИДны көрө албашын камсыз кылууга милдеттүү.

6.8. ИСУО менен иштөө аяктагандан кийин, кызматкерлер жумушчу станцияны ачык калтыруу же эквиваленттүү баалкаруу менен коргоого милдеттүү. мисалы, күчтүүрөөк коргоо каражаттары колдонулбаса.

6.9. Кызматкерлери ИД коопсуздук режимин бузуу коркунучу жана аны бузгандыгы үчүн жоопкерчилик жөпүндө маалымдалышы керек. Алар ИДнын коопсуздугунун саясатын жана жол-жоболорун бузган кызматкерлерге тартиптик жаза колдонуунун бекитилген расмий тартиби менен таанышууга тийиш.

6.10. Кызматкерлер ИДнын коопсуздугун коркунуч келтириши мүмкүн болгон ISPD илинин бардык байкалган жер шектүү учурлары жөпүндө, ошондой эле алар аныктаган ИДнын коопсуздугуна, ОСтун жетекчилиги менен жана ИДнын коопсуздугуна коркунучтарга дароо жооп кайтаруу үчүн жооптуу адам.

7. Интернетти колдонуу.

7.1. Өз бөлүмчө интернетти пайдалануу окуу процессинин максаттарында ишке ашырылат.

Инсандын өнүгүүсүнүн, анын социалдаштырылышынын жана компьютердик сабаттуулук жаатындагы билимдердин бир бөлүгү катары адам билим берүү эмес ресурстарга кире алат.

7.2. Түдө Интернетти колдонуу төмөнкү принциптерге баам ийет:

- билим берүү максаттарына ылайык келүү;
- инсандын гармониялуу калыптанышына жана өнүгүшүнө салым кошуу;
- автордук жана чектеш укуктар жөнүндөгү мыйзамдарды, ошондой эле башка жарандардын жана интернет колдонуучулардын башка укуктарын, ар-намысын жана калтыр-баркын сыйлоо;
- жаңы көндүмдөрдү жана билимдерди алуу;
- колдонулуучу окуу жана көрсөтмө куралдардын спектрин кеңейтүү;
- инсанды социалдаштыруу, маалыматтык коомго киргизүү.

7.3. Сабак учурунда окуучулардын Интернетти утуу эрежелерге ылайык пайдаланышын контролдоо сабактын анын баруучу мугалим тарабынан ишке ашырылат.

Окуу процессинде мугалим:

- окуучулардын компьютерлерди жана интернетти колдонуусун көзөмөлдөйт;
- өгөрдө студент бул эрежелерди жана билим берүү мекемесинде Интернетти колдонууну жөнгө салуучу башка ченемдик документтерди бузса, студенттин Интернетте андан ары иштөөсүнө тыюу салат;
- билим берүүнүн максаттарына ылайык келбеген ресурска/ресурс ардык тобуна кирүү аракеттерин болтурбоо үчүн утуу эрежелерде жана башка ченемдик укуктук документтерде каралган чараларды көрөт;
- балдарда маалыматтык продуктыларды өз алдынча жана жоопкерчиликтүү керектөө көндүмдөрүн калыптандырат;
- балдардын өнүгүүсүнө баалуулук, моралдык жана моралдык-этикалык алып келет;
- маалыматтык коомсуздукту камсыз кылуу фактору катары маалыматтык маданиятты калыптандырат.

7.4. ИКОНун кызматкерлери төмөнкүлөргө укуктуу:

Интернетте жайгаштырылган ресурстарды, анын ичинде КБНБ интернет-ресурстарын

ушул Регламентте каралган.

- БЗнын интернет-ресурстарына маалыматты жана маалыматтарды жайгаштыруу.
- ООдо маалыматташтыруу тармагында юридикалык билимдерди алуу.
- компьютеризди зыяндуу программалардан, мыйзамсыз, параттык мазмундан жана аны жүктөп алуу коркунучтарынан коргоо жөнүндө билимге ээ болуңуз.

8. Окуучуларга төмөнкүлөргө тыюу салынат.

8.1 Мазмуну жана предмети жашы жетишендер үчүн алгылыксыз белгилон жана/же Кыргыз Республикасынын мыйзамдарын бузган ресурстарга барушу, атап айтканда:

- окуучуларга алардын өмүрүнө жана (же) ден соолугуна коркунуч туудурган, анын ичинде ден соолугуна зыян келтирген аракеттерди жасоого үндөгөн;

- окуучуларга баңги каражаттарын, психотроптук жана (же) мас кылуучу заттарды, тамеки буюмдарын, алкоогодук жана алкоогодук продукцияны колдонууга тыюу салынат;

- зомбулукка жана (же) ырайымсыздыкка же адамдарга же жаныбарларга карата зомбулук аракеттерди жасоого чыккандыруучу аракеттерге жол бериле тургандыгын негиздеген же айткан,

үй-бүлөлүк баалуулуктарды четке кагуу.

- мыйзамсыз жүрүм-турумду актөө;

- Интернет аркылуу ар кандай транзакцияларды жүргүзүүгө;

- жооптуу адамдын уруксатысыз өз компьютеринин файлдарды жүктөөгө;

- башка адамдардын кадыр-баркына шек келтирүүгө, чындыкка дал келбеген маалыматтарды, коркутууларды таратууга.

- экстремизмди жана жалпы кабыл алынган нормалардан четтеген жүрүм-турум формаларын пропагандалаган сайттарга баруу.

8.2. интернет колдонуучулар техникалык каражаттар жана программалык камсыздоо ресурстарды тез-тез жаңыртуудан улам интернет-ресурстарды толук чыпкалоону камсыз кыла албастыгын эске алуулары керек. Ушуга байланыштуу окуучулардын мазмуну Кыргыз Республикасынын мыйзамдарына карама-каршы келген жана ОО интернет-ресурстарынан эмес, окуу процессинин максаттарына жана милдеттерине туура келбеген

ресурстарды табуу коркунучу бар. Интернетти колдонуунун катышуучулары башка интернет-ресурстарга жайгаштырылган мындай маалыматтарга кокусан жетүү үчүн

мектеп жооптуу эмес экенин билиши керек.

8.3. Эгерде колдонуучу иштин жүрүшүндө мазмуну билим берүү процессинин максаттарына

туура келбеген ресурсу гана, ал интернет дарегин (URL) көрсөтүү менен бул тууралуу дароо жооптуу адамга билдирүүгө жана бул ресурстан чыгып кетүүгө милдеттүү.

9. Маалыматтык коопсуздукту камсыз кылуу үчүн жооптуу адамдардын укуктары.

9.1. Мектептин кызматкерлеринен белгиленген технологияны шартсыз аткарууну жана чектелген маалыматты камтыган маалыматтык коопсуздугун жана коргоону камсыз кылуу боюнча нускамаларды аткарууну талап кылуу.

9.2. Маалыматтык коопсуздук системасын өркүндөтүү боюнча сунуштарды даярдоо үчүн.

10. Маалыматтык коопсуздук үчүн жооптуу адамдардын жоопкерчилиги.

10.1. Маалыматтык коопсуздук үчүн жооптуу адамдар маалыматтык коопсуздукту камсыз кылуу боюнча иштин сапаты үчүн, маалыматты коргоону ушул Жободо аныкталган функционалдык милдеттерге ылайык жеке жоопкерчилик тартышат.