Õpilaste IT-teenuste kasutamise kord

Jõgevamaa Gümnaasium

Sisukord

1. Sissejuhatus

1.1. Õpilaste IT-teenuste kasutamise kord (edaspidi kord) on Jõgevamaa Gümnaasiumi (edaspidi kool või asutus) infoturbe korra lisa, mis sätestab kooli IT-teenuseid kasutavate õpilaste (edaspidi kasutaja) õigused ja kohustused IT-varaga töötamisel ja teabe töötlemisel. IT-teenuste kasutamise korra eesmärk on aidata kaasa kooli infovarade konfidentsiaalsuse, tervikluse ja käideldavuse tagamisele ning toetada kooli üldisi infoturbe eesmärke, nagu sätestatud infoturbe kontseptsioonis.

1.2. Kord vaadatakse üle perioodiliselt, aga vähemalt 1 kord aastas, ning pärast oluliste muudatuste tegemist IT-süsteemides. Korra ajakohastamise korraldab infoturbejuht või tema poolt määratud töötaja.

1.3. Kasutaja on kohustatud täitma käesoleva korra nõudeid ning peab tegutsema vastutustundlikult. Kooli IT-teenuse kasutamise korral eeldatakse, et kasutaja on tutvunud kehtiva korra nõuetega.

1.4. Käesoleva korra tutvustamise kasutajale korraldab infoturbejuht. Uus kasutaja kinnitab enne IT-vahendite kasutuselevõttu kooli sisseastumiseinfosüsteemis kirjalikult, et on eeskirjaga tutvunud.

2. Mõisted

2.1. Eeskirjas kasutatakse mõisteid järgmises tähenduses:

Mõiste	**Selgitus**
Andmed	Teabe ehk informatsiooni taastõlgendatav esitus formaliseeritud kujul, mis sobib edastuseks, tõlgenduseks või töötluseks. Andmed hõlmavad mis tahes viisil ja mis tahes andmekandjatele jäädvustatud või dokumenteeritud teavet ning kõigi sh infotehnoloogiliste vahendite abil edastatavat või töödeldavat teavet. Andmed on jaotatud tundlikkuse järgi rühmadesse, milledele kehtivad erinevad salastusnõuded.
Arvutivõrk	Kogum erinevatest andmesideseadmetest, mille kaudu on arvutid, printerid, serverid, nutitelefonid ja teised seadmed andmevahetuse või ressursside jagamise eesmärgil omavahel ühendatud.
Intsident	Sündmus, mis tegelikult või potentsiaalselt ohustab ilma seadusliku volituseta teabe või infosüsteemi konfidentsiaalsust, terviklust või kättesaadavust; või kujutab endast turvapoliitika, turbeprotseduuride või vastuvõetava kasutuse poliitika rikkumist või vahetut ohtu rikkuda,

	põhjustades võimaliku kahju või häire asutuse infosüsteemide toimimises.
Irdseade	Seade, mida lõppkasutaja saab oma tavapärase töö käigus süsteemiga ühendada või sealt eemaldada, nt USB-mälupulk. Info ja kommunikatsioonitehnoloogilise seadme väline andmekandja, mida lõppkasutaja saab oma tavapärase töö käigus süsteemiga ühendada, näiteks mälupulgad, välised kõvakettad, mälukaardid ja CD/DVD/BR -plaadid
IT-teenused	Infotehnoloogilised seadmed ja süsteemid (arvutid, printerid, serverid, võrguühendused, tarkvara jms) ning nende kasutamist tagav töökorraldus
Kasutaja	Asutuse töötaja või väline kasutaja, kellele tööülesannetest või muudest vajadustest tulenevalt on antud õigused asutuse IT-teenuste isikuandmete töötlemise ja väliste andmekandjate kasutamiseks
Kasutajatunnus, kasutajakonto	Pääsuõiguse tunnus, mis annab kasutajale pärast salasõna sisestamist õiguse juurde pääseda piiratud andmetele ja ressurssidele.
Monitoorimine	Protsess, mille käigus jälgitakse ja hinnatakse süsteemi, teenuse või tegevuse jõudlust ja turvalisust. Monitoorimise eesmärk on tuvastada ja reageerida võimalikele probleemidele, ohtudele või kõrvalekalletele varases staadiumis, et tagada süsteemide katkematu ja turvaline toimimine.
Pilverakendus	Interneti kaudu kasutatav tarkvara, mis töötab väljaspool asutuse vahetut kontrolli olevas kaugserveris.
Salasõna	Salajane märgijada, millega tõestatakse oma isikusamasust arvutisüsteemi või rakendusse sisenemisel.
Turvanõrkus	Viga tööprotsessis või arvutirakenduses (sh konfiguratsioonis), mida on saab kuritarvitada pahatahtlikel eesmärkidel, näiteks arvutisüsteemile ligi saamiseks või info hankimiseks.

3. Kasutaja üldised kohustused

3.1. Kasutaja kohustub:

3.1.1. **kasutama ja kaitsma temale määratud kasutajatunnuseid, sh**

3.1.1.1. asendama talle antav esmane salasõna (parool) esimesel sisselogimisel;

3.1.1.2. hoidma saladuses oma kasutajatunnust ja salasõna (parool), mitte jagama neid teistega;

3.1.1.3. kasutama erinevates infosüsteemides ja internetikeskkondades erinevaid paroole ning mitte kasutama varem kasutusel olnud paroole, enda ja oma lähedaste isikuandmeid või muid seotud andmeid st välistama kasutaja isiku identifitseerimise võimaluse;

3.1.1.4. kasutama parooli, mis on vähemalt kümme tähemärki pikk, sisaldab suur- ja väiketähti ning numbreid, kirjavahemärke või muid sümboleid. Soovitavalt kasutama täiendava turvameetmena kaheastmelist autentimislahendust infosüsteemides, kus see on saadaval;

3.1.1.5. vahetama oma parooli vähemalt 1 kord aastas;

3.1.1.6. teavitama koheselt IT-juhti või infoturbejuhti ning vahetama esimesel võimalusel parooli, kui see on saanud teatavaks teistele isikutele või on tekkinud sellekohane kahtlus;

3.1.1.7. mitte kasutama teiste kasutajate kasutajatunnuseid;

3.1.2. **kaitsma kooli andmeid ja vara**, sh

3.1.2.1. vältima andmete lubamatut levitamist, s.h. kooli teiste õpilaste isikuandmete levitamist;

3.1.2.2. kaitsma oma käsutusse antud asutuse vara, sh tagades nende järelevalve;

3.1.2.3. tagama, et kõrvalistel isikutel ei oleks võimalik kirjutada tema failikataloogidesse ega failidesse;

3.1.2.4. tagama kooli vara ja andmete kaitstuse nende kasutamisel väljaspool kooli arvutivõrku;

3.1.3. **olema vastutustundlik**, sh

3.1.3.1. järgima turvanõudeid;

3.1.3.2. andma esimesel võimalusel infoturbejuhile või IT-juhile teada kõigist turvarikkumistest ning leitud turvanõrkustest;

3.1.4. **austama teiste õiguseid**, sh

3.1.4.1. kasutama teiste andmeid ja intellektuaalset omandit vaid legaalsel viisil;

3.1.4.2. mitte takistama teiste kasutajate õiguspäraseid tegevusi;

3.2. **Kasutajal on õigus:**

3.2.1. saada õppetööks juurdepääsuõigus IT-teenustele, milleks antakse kooli poolt personaalne kasutajakonto koos privaatse kettaruumiga failiserveris ning e-posti aadress;

3.2.2. pöörduda infoturbe- ja andmekaitsealastes küsimustes infoturbejuhi poole;

3.2.3. kasutada IT-vara vastavalt õppeeesmärkidele;

3.2.4. saada IT-varaga töötamisel abi IT- juhilt;

3.2.5. saada teabe turvalise töötlemise ja IT-varaga töötamise alaseid koolitusi;

3.2.6. saada teavet muudatustest ja sündmustest, mis on seotus IT-vara kasutamisega ja teabe turvalise töötlemisega.

4. Üldised kasutustingimused

4.1. Kooli IT-vara ja teave on ette nähtud kasutamiseks kooskõlas asutuse eesmärkidega.

4.2. Kasutaja vastutab enda kasutajakontoga infosüsteemis ja arvutivõrgus tehtud toimingute (sh erinevate internetilehekülgede, sotsiaalmeedia, suhtlusportaalides tehtavad toimingud) ja infosüsteemi sisestatud andmete õigsuse eest.

4.3. Kool võib jälgida (monitoorida) kõigi kasutajate tegevust asutuse IT-seadmetes, IT-süsteemides ja arvutivõrkudes, ning võib vajadusel piirata või tõkestada kasutaja tegevust või selle tulemusel toimuvat andmete liikumist.

4.4. Kasutaja teatab viivitamatult kooli IT-vara või teabega seotud kahjulikest sündmustest või eeskirjade rikkumistest (intsident) IT-juhti (email: kool@gymnaasium.ee, tel 5681 3034) või infoturbe kontaktisikut.

4.5. Intsidendi uurimisel on kasutaja kohustatud aitama kaasa juhtunu selgitamisele. Õpilane on kohustatud teatama infoturbeintsidendist või haavatavusest ning aitama uurimisel kaasa juhtunu selgitamisele.

5. Turvakoolitus ja teadlikkus

5.1. G1 õpilased läbivad õppeaasta alguses enesetesti RIA testide põhjal. G2 ja G3 õpilastele edastatakse vastav teave või info õppeaasta alguses mentortunni raames.

6. Tarkvara ja riistvara

6.1. Kasutaja vastutab tema valduses oleva asutuse vara eest.

6.2. Kasutajale tööülesannete täitmiseks antud riist- ja tarkvara tuleb kasutada õppe-eesmärgil.

6.3. IT-varade tervikluse ja turvalisuse säilitamiseks ning haavatavuste või pahavara sisseviimise vältimiseks ei ole kasutajal lubatud installeerida täiendavat riist- või tarkvara tööarvutisse ilma IT-juhi loata, välja arvatud automaatsed tarkvara täiendused ja uuendused, ühendada uut riistvara

asutuse sisevõrku ning seadmeid sisevõrgus ümber paigutada, välja arvatud sülearvutid.

6.4. Kasutaja kohustub viivitamatult teavitama kooli personali infotehnoloogiliste seadmetega seotud probleemidest.

7. Juurdepääsuõigused

7.1. Kasutaja vastutab isiklikult oma kasutajatunnusega teostatud toimingute eest.

7.2. Esmasel sisselogimisel infosüsteemi peab kasutaja ära muutma IT-juhi poolt antud salasõna. Salasõna tuleb sisestada kõrvalistele isikutele märkamatult. Salasõna peab koosnema soovitavalt vähemalt 10-st tähe-numbri kombinatsiooni moodustavast sümbolist ning välistama kasutaja isiku identifitseerimise võimaluse.

7.3. Kui on tekkinud kahtlus, et salasõna on saanud teatavaks kõrvalistele isikutele, tuleb viivitamatult kasutusele võtta uus salasõna.

7.4. Arvutiklassis arvuti tagant lahkudes peab kasutaja end arvutist välja logima või kasutajakonto ajutiselt lukustama.

8. Andmeturve

8.1. Füüsilisel viisil edastatav konfidentsiaalne teave peab olema kaitstud kooskõlas kooli nõuetega. Konfidentsiaalse teabe füüsilise edastamise korral peab seda tegema isiklikult või kasutama asutuse poolt heakskiidetud kullerteenust.

8.2. Konfidentsiaalse või siseteabe jagamiseks, salvestamiseks ja edastamiseks digitaalselt võib kasutada ainult kooli poolt lubatud IT teenuseid ja pilverakendust (Office 365).

8.3. Teavet tuleb käsitleda vastavalt tema tundlikkusele, sh jagada, käsitseda, edastada, salvestada ja hävitada.

8.4. Kasutaja ei tohi pidada konfidentsiaalseid vestlusi avalikes kohtades, avatud kontorites ja kohtumispaikades või ebaturvaliste sidekanalite kaudu.

8.5. Kõik konfidentsiaalset teavet sisaldavad elektroonilised andmekandjad tuleb peale kasutuse lõppu turvaliselt kõrvaldada kooskõlas kooli poolt kehtestatud nõuetega.

9. Irdseadmete kasutamine

9.1. Kasutaja isiklike sh teiste asutuste poolt antud irdseadmete kasutamine kooli poolt väljastatud IT-vahendites on keelatud.

10. Internet

10.1. Kasutaja on kohustatud interneti kasutamisel tegutsema legaalselt ning lähtuma üldkehtivatest eetikanormidest ja isiku eraelu puutumatuse põhimõttest. Kasutaja vastutab interneti kaudu edastatud info eest.

10.2. Interneti kasutamine ebasündsatel eesmärkidel, samuti tundmatute ja illegaalsete failide allalaadimine või käivitamine on keelatud.

10.3. Interneti kasutamisel sülearvutis avalikes traadita võrkudes tuleb arvestada võimalusega, et võrk on ebaturvaline ning edastatav info võib sattuda kõrvaliste isikute valdusesse.

11. E-post ja OneDrive

11.1. Kasutaja õppima asumisel loob kool talle personaalse kasutajakonto koos privaatse pilveruumiga (OneDrive) ning e-posti aadressi. Koolist lahkumisel kasutajakonto ja e-posti aadress suletakse 1 tööpäeva jooksul.

11.2. E-posti aadress ja OneDrive on antud personaalseks kasutamiseks ainult õpetööks vajaliku teabe töötlemiseks. Keelatud on edastada e-posti ja hoida OneDrive’s faile, mille sisu on illegaalne, ebaeetiline, seotud isikliku tulu teenimisega või kahjustab kooli mainet.

11.3. E-posti lugemiseks ja saatmiseks tuleb kasutada kooli poolt seadistatud tarkvara või asutuse e-posti veebiteenust.

11.4. E-posti ja OneDrive ressursi tahtlik raiskamine või muu tegevus, mis häirib süsteemi kasutust asutuse poolt määratud otstarbel, on keelatud. E-posti manuse maksimaalne lubatud suurus on 25 megabaiti, mida vajadusel suurendatakse.

11.5. Kasutaja on kohustatud regulaarselt korrastama oma e-posti ja OneDrive’s asuvaid andmeid, kustutades või arhiveerides ebaolulised kirjad ja failid.

12. Viirustõrje

12.1. Viiruse või ründetarkvara kahtlusega e-posti manuste, veebilehtede, failide ning internetiviidete avamine on keelatud.

12.2. Viiruse või ründetarkvara avastamisel tuleb viivitamatult teavitada kooli personali ning seisata oma töö arvutis kuni IT-juhilt loa saamiseni töö jätkamiseks.

12.3. Arvutite, serverite ja andmekandjate teadlik nakatamine viiruste või ründetarkvaraga on keelatud, samuti automaatse taustkontrolli väljalülitamine, viirustõrjeprogrammide määrangute muutmine ning aktiveerunud ründetarkvara omaalgatuslik eemaldamine.

13. Sülearvutid

13.1. Mobiilsete seadmete (sülearvutid, välised kõvakettad, mälupulgad jms) järelevalveta jätmine ning muul moel kõrvalistele isikutele volitamata ligipääsu võimaldamine on keelatud.

13.2. Mobiilsete seadmete ja andmekandjate rikkumisest või kadumisest tuleb koheselt teavitada kooli personali.

13.3. Õppetööks väljastatakse õpilasele pikemaks perioodiks (rohkem, kui 1 päev) eraldi kokkuleppe alusel ja vajadusel seadmed ja selle turvalisuse eest vastutab kasutaja.

12.3.1. Kasutajal on keelatud ühendada sülearvuteid avalikku wifi-võrku, kui see on parooliga kaitsmata, eelistades andmesideühendusega pakutavat internetiühendust või enda mobiiltelefoniga tehtavat kuumkohta (hotspot).

13.4. Õppetööks väljastatud sülearvutitele tohib uusi rakendusi lisada ja vanu eemaldada ainult IT-juhiga kooskõlastusel.

14. Kasutajatunnuste sulgemine

14.1. Õpilase koolist väljaarvamisel peab kasutaja:

14.1.1. eemaldama oma isiklikud andmed kooli seadmetest;

14.1.2. tagastama kasutaja valduses olevad kooli IT-varad oma mentorile.