Politica de Utilizare Acceptabilă (PUA)

POLITICA eSAFETY A ȘCOLII

ȘCOALA GIMNAZIALĂ „ELENA DOAMNA” TECUCI, JUD. GALAȚI

Fiind vorba de o organizație profesională responsabilă cu protejarea copiilor, este important ca întregul personal să ia toate măsurile posibile și necesare pentru a proteja sistemele de date și informații împotriva infectării, accesului neautorizat, pagubelor, pierderilor, abuzului și furtului. Toți membrii personalului au responsabilitatea de a utiliza sistemul informatic al școlii în mod profesional, legal și etic. Mai mult, politica BOYD *Bring your own device* (aducerea propriului dispozitiv de acasă) este adoptată astăzi în multe școli, ceea ce face ca problemele de protecție și de securitate să fie și mai dificile. Pentru a garanta că sunt pe deplin conștienți de responsabilitățile lor profesionale atunci când folosesc Tehnologiile Informaţionale şi de Comunicare membrii personalului sunt rugați să citească și să semneze Politica de Utilizare Acceptabilă.

Această listă nu este una exhaustivă și tuturor membrilor personalului li se reamintește că utilizarea TIC trebuie să fie în concordanță cu etosul școlii, cu alte politici adecvate și cu legea.

UTILIZAREA TELEFOANELOR MOBILE ÎN ȘCOLI

A devenit din ce în ce mai dificil de pus în aplicare o interdicție absolută cu privire la utilizarea telefoanelor mobile în școli, pe de-o parte deoarece acestea au devenit indispensabile în viața tinerilor, dar şi pentru că mulți părinți insistă să poată intra în orice moment în legătură cu copiii lor. Deși prezența telefoanelor mobile poate fi deranjantă și poate conduce la comportamente deranjante precum copierea şi bullyingul, ele pot, de asemenea, să ofere oportunități fără precedent atunci când sunt utilizate în mod proactiv și creativ în sala de clasă, atâta timp cât există o politică strictă privind deținerea și utilizarea acestora

- Reţeaua Wi-Fi a şcolii nu este accesibilă pe telefoanele mobile, dar poate fi accesată de către elevi, pe cea separată de reţeaua securizată destinată personalului / activităţilor principale (router wi-fi instalat în clasă).
- În cazul confiscării unui telefon mobil, elevul trebuie să oprească telefonul înainte de a-l înmâna profesorului, pentru a asigura protecţia datelor personale de pe telefon. Dacă telefonul nu este returnat la sfârşitul orelor de curs, părinţii ar trebui să fie informaţi şi telefonul mobil trebuie să fie păstrat într-un loc sigur .
- Părinţii sunt informaţi cu privire la politica referitoare la utilizarea telefonului mobil, cu privire la motivele pentru care sunt luate aceste măsuri şi cu privire la posibilele consecinţe pe care le poate implica o încălcare a acestei politici.

UTILIZAREA DISPOZITIVELOR DETAŞABILE

Dispozitiv detaşabil înseamnă orice dispozitiv media care poate fi citit şi/sau inscripţionat de către utilizatorul final şi mutat de la un computer la altul fără să producă modificări computerului respectiv. Printre aceste tipuri de dispozitive se numără aparatele ce conţin memorii flash, cum ar fi aparate foto, MP3 playere, hard disk-uri portabile, CD-uri, DVD-uri şi stick-uri USB. Utilizarea dispozitivelor de stocare detaşabile este o sursă bine-cunoscută de infecţii malware şi este direct legată de scurgerea de informaţii sensibile în multe organizaţii. Este necesar să se ia măsuri corespunzătoare pentru a reduce la minimum riscul de scurgere sau de expunere a informaţiilor sensibile şi pentru a reduce riscul infecţiilor malware pe computerele şcolii.

- În cadrul Politicii de Utilizare Acceptabilă sunt dezvoltate reguli de bază privind folosirea dispozitivelor detaşabile de stocare pe computerele şcolii.
- Este instalat un sistem de protecţie antivirus pe toate computerele din reţeaua şcolară şi se adoptă o practică constantă la nivel de şcoală în ceea ce priveşte protecţia împotriva virusilor. Un fişier infectat de pe un dispozitiv de stocare amovibil ar putea infecta întreaga reţea şcolară.
- Se solicită membrilor personalului şi elevilor să scaneze toate dispozitivele detaşabile împotriva programelor malware înainte de a le utiliza.
- Se permite utilizarea dispozitivelor mobile numai când sunt necesare în vederea îndeplinirii sarcinilor şcolare. Elevilor şi membrilor personalului nu trebuie să li se permită, de exemplu, să-şi conecteze aparatul foto sau un MP3 player-ul la un computer din reţeaua şcolii, cu excepţia cazului în care trebuie să facă acest lucru în cadrul unei sarcini specifice pe care au primit-o.
- Se încurajează personalul şi elevii să salveze fişiere pe dispozitivele mobile pe care le folosesc pe computerele şcolii doar în scopuri educaţionale .
- Personalul trebuie să evite stocarea datelor sensibile ale elevilor şi ale altor membri ai personalului pe dispozitive detaşabile cu excepţia cazului în care acest lucru este

necesar în vederea executării sarcinilor ce le revin, deoarece există întotdeauna riscul ca aceste dispozitive cu informații personale pe ele să fie furate sau pierdute.

- Este instituită o procedură oficială de gestionare a incidentelor în cazul unor infectii malware prin utilizarea unui dispozitiv mobil sau în cazul pierderii unui dispozitiv. Aceasta din urmă este deosebit de importantă dacă dispozitivul conține informații sensibile despre elevi sau personal.

PROTEJAREA DATELOR SENSIBILE ÎN ŞCOLI

Datele sensibile din cadrul unei şcoli includ detaliile confidenţiale ale elevilor, părinţilor şi membrilor personalului, informaţiile şcolare, de sănătate şi psihologice ale elevilor, salariile profesorilor şi CV-urile acestora, precum şi date privind administrarea şcolii. Aceste informaţii pot fi stocate pe computerele locale, pe dispozitive mobile, pe servere localizate pe teritoriul şcolii sau în alte locaţii sau pe documente printate pe o imprimantă confidenţială sau comună. Protecţia insuficientă sau dezvăluirea improprie a acestor date poate rezulta într-o încălcare a confidenţialităţii sau a legilor de protecţie a datelor.

- Se actualizează sistemele de protecţie antivirus pentru a evita să deveniţi o țintă a hackerilor.
- Inginerie socială [1] reprezintă cel mai mare risc de securitate; se discută cu personalul din şcoală pentru asigurarea că aceştia nu se lasă păcăliţi în oferirea de date.
- Nu lăsați documente ce conţin date sensibile pe imprimanta publică sau salvate pe calculator! Distrugeţi / stergeți astfel de documente înainte să le puneţi în coşul de gunoi (Recycle Bin).
- Colectaţi date sensibile doar dacă este necesar. Ceea ce nu deţii, nu poate fi compromis!

[1]*Ingineria socială se referă la comunicări (prin intermediul site-urilor sau emailurilor) care păcălesc utilizatorul să viziteze un site web sau să execute click pe o legătură pentru a deschide un ataşament care oferă acces la informaţii confidenţiale.*

PROTECȚIA DISPOZITIVELOR ÎMPOTRIVA PROGRAMELOR MALWARE

Malware înseamnă software dăunător care a fost proiectat cu scopul accesării unei rețele sau unui sistem de computere fără consimțământul proprietarului și poate include viruși, viermi și spyware. Odată instalat, malware-ul cauzează de obicei rezultate nedorite, care pot varia de la a fi pur și simplu intruziv sau enervant până la a compromite informații cu caracter personal în sistem sau până la a fi pur și simplu distructiv. Malware-ul ajunge de obicei în sistemul IT al unei școli prin intermediul spam-ului, descărcării de fișiere

contaminate sau prin intermediul dispozitivelor mobile infectate (USB, hard disk extern, telefon mobil, etc.).

- Pe fiecare calculator este instalat firewall-ul și sisteme de protecție anti-virus și se actualizează pentru a evita breșele de securitate.
- Se blochează site-urile nedorite și ferestrele de tip pop-up prin personalizarea setărilor de securitate ale browser-ului web utilizat pe computerele școlii. Se explică elevilor de ce anume se face acest lucru și se precizează că prin aceasta se urmărește protecția lor.
- Se creazăi un protocol care să fie aplicat cu rigurozitate cu privire la utilizarea Internetului și verificarea mail-urilor personale pe computerele școlii.
- Nu se accesează din mailuri adrese dubioase / reclame / pop-up orice ce nu au legătură cu activitatea școlară.
- Nu se permite elevilor să folosească dispozitive portabile pentru a descărca fișiere de pe computerele școlii; în cazul în care acest lucru este permis trebuie să fie instruiţi să scaneze mai întâi toate fișierele împotriva malware.
- Se desemnează o persoană de contact instruită să se ocupe de toate problemele legate de malware și se instituie o procedură oficială de gestionare a incidentelor informatice.

POLITICA DE UTILIZARE ACCEPTABILĂ (PUA)

Reprezintă o bună practică ca toate şcolile să aibă o Politică de Utilizare Acceptabilă (PUA), adică un document clar şi concis care să ofere îndrumare unor categorii de utilizatori cu privire la felul în care ar trebui utilizate Internetul şi tehnologiile mobile.

Politicile de Utilizare Acceptabilă s-au dezvoltat în timp şi este evident că tinerii şi personalul din şcoli au posibilitatea să acceseze Internetul în multe moduri, nu numai prin intermediul reţelei şcolii. Având în vedere acest fapt, este important ca o Politică de Utilizare Acceptabilă să fie centrată mai mult pe comportament decât pe tehnologie. Acest lucru înseamnă că politica va avea o viaţă mai lungă şi va fi mai uşor de înţeles de către toţi cei interesaţi.

PAROLE SIGURE

Parolele oferă puncte unice de intrare în sistemul școlar de computere și trebuie aplicate cu rigurozitate câteva reguli de bază referitoare la securitatea acestora.

- Se amintește personalului și elevilor cele 4 reguli de aur ale unui parole sigure:
    1. Trebuie să fie lungă și complexă.Ideal trebuie să conţină între 10 și 14caractere ;
    2. Se folosește un amestec de numere, simboluri, litere mari şi litere mici și semne de punctuație ;

3. Se foloseşte metode mnemonice care să vă ajute să vă amintiţi parola, de exemplu un acronim pentru o frază, cum ar fi "Fiica mea, Harriet, este o bună jucătoare de tenis" devine FMhEObjDt sau Imi place să cânt in ploaie in fiecare zi! devine iPScipIFZ !;
4. Nu folosiți niciodată informații personale de identificare în parolă. Acestea includ nume, zile de naștere, animale de companie, adrese de străzi, şcoli, numere de telefon, numerele de înmatriculare etc. Acestea vor fi primele presupuneri pentru oricine încearcă să obțină acces la contul dvs.

- O parolă este ca o periuță de dinţi, nu trebui folosită în comun şi trebuie să fie schimbată frecvent!
- Dacă utilizatorii simt totuşi nevoie să scrie parola, aceasta nu trebuie să fie ţinută în apropierea dispozitivului la care oferă acces.

POLITICA ŞCOLII

Politicile de eSafety ale şcolii s-au dezvoltat rapid, deoarece părțile interesate pot accesa în prezent Internetul într-o multitudine de moduri în incinta şcolii. Tehnologiile digitale fac parte din viața noastră de zi cu zi. Pentru a ne asigura că oportunitățile disponibile prin intermediul tehnologiilor digitale sunt valorificate cum se cuvine de către copiii noştri, aceştia trebuie să le cunoască şi să înțeleagă cum să le folosească, acum mai mult ca niciodată. Pentru a ne asigura că acest lucru se face în cel mai sigur mediu posibil, fie acasă, fie la şcoală sau când ies în oraş singuri sau cu prietenii lor, toate şcolile trebuie să aibă o politică clară şi concisă în care să se acorde atenție tuturor aspectelor eSafety.

REALIZAREA ŞI PUBLICAREA DE FOTOGRAFII ŞI CLIPURI VIDEO ÎN CADRUL ŞCOLII

Participarea copiilor într-un concert sau într-o piesă de teatru la şcoală este un moment de neuitat şi un motiv de mândrie pentru părinți – este un moment pe care mulți vor dori să-l fotografieze sau să-l filmeze. Având în vedere accesul rapid de la un ecran de telefon mobil la un site de socializare, există anumite reguli pe care conducerea şi personalul şcolii ar trebui să le ia în considerare şi să le comunice părinților.

- Se asigură că şcoala are o politică clară referitoare la imagine şi fotografie indiferent dacă aceasta este sau nu o obligație legală în țara dvs.
- Se comunică comunității şcolare această politică alături de îndrumări practice clare şi exemple uşor de înțeles.
- Se asigură că toți părinții/tutorii legali şi/sau tinerii (în funcție de vârstă şi cerințe naționale) au semnat un fomular de permisiune pentru foto/video ÎNAINTE de orice filmare sau fotografiere a elevilor.

- Dacă părintele/tutorele nu-şi dă acordul, înţelegeţi posibilul disconfort al elevului respectiv şi aranjaţi discret ca el/ea să aibă o altă ocupaţie în timpul procesului de filmare sau fotografiere.
- Se asiguraă că toţi membri comunităţii şcolare înţeleg implicaţiile partajării fotografiilor şi conţinutului video pe site-urile de socializare – nu postaţi NICIODATĂ numele complet, vârsta sau orice alte detalii personale alături de fotografia unui copil pe site-ul dvs.!
- Ţineţi minte că evenimentele şcolare sunt ocazii de bucurie care nu ar trebui să fie restricţionate de prea multe reglementări.

PREZENŢA ŞCOLII PE REŢELELE DE SOCIALIZARE

Folosirea reţelelor de socializare de către şcoli este un subiect controversat, putând fi aduce argumente pentru şi împotrivă, de la riscul cyberbullying-ului şi prieteniile online dintre elevi şi profesori până la promovarea activă pe care o poate aduce Facebook sau Twitter.De la dezvoltarea profesională până la descoperirea de exemple din viaţa reală la orele de limbi străine, socializarea media în şcoli poate reprezenta o resursă valoroasă. Cel mai important lucru care trebuie avut în vedere în legătură cu utilizarea reţelelor de socializare în şcoli este chestiunea drepturilor şi responsabilităţilor online.

Pe lângă rolul de intrument promoţional pentru şcoli, profesorii din toată lumea au enumerat mai jos beneficiile utilizării reţelelor sociale în şcoli.

- Dezvoltarea profesională în ceea ce priveşte utilizarea instrumentelor tehnice şi de social media pentru profesori.
- Utilizarea unor metode de învățare moderne, incluzive și alternative.
- Informarea și sensibilizarea comunității și a părinților prin intermediul grupurilor de Facebook, Pinterest, Yammer, Twitter și altele.
- Comunicarea cu părinții în cazul în care sunt prieteni pe Facebook cu școala/clasa/ proiectul școlar.
- Comunicarea interculturală cu alte școli.
- Învățarea limbilor străine.
- Învățarea colaborativă și împărtășirea de informaţii cu colegi și grupuri educaţionale cu aceleaşi interese.
- Stabilirea de legături cu colegi din întreaga țară și chiar din lume.
- Integrarea unor exemple din lumea reală în procesul de predare.

  ✓ **Reţeaua de socializare Facebook este restricţionată în sălile de clasă unde se desfăşoară orele de curs.**

INTEGRAREA ESAFETY ÎN CURRICULUM

Deşi TIC şi mediul digital oferă copiilor şi adolescenţilor un potenţial enorm de a explora, de a se conecta şi de a crea, elevii au nevoie de îndrumări suplimentare cu privire la comportamentul sigur şi responsabil în mediul online. În special, ei trebuie să înveţe strategii eficiente de găsire a unui echilibru între oportunităţi şi riscuri, de gestionare a informaţiilor online şi a securităţii acestora, de protejare a intimităţii lor şi respectare a celuilalt, de gestionare a cazurilor de cyberbullying, de a distinge între contacte şi conţinut nepotrivit şi pozitiv, ş.a.m.d.

- Se asigură că eSafety se predă ca parte a programei, indiferent dacă aceasta este sau nu o obligaţie legală în ţara dvs.
- Deşi predarea eSafety în cadrul cursurilor de TIC sau media pare cea mai potrivită abordare, şcoala ar trebui să urmărească o abordare trans-curriculară mai cuprinzătoare, care explorează numeroasele legături dintre eSafety şi toate tipurile de conţinut educaţional.
- Deoarece eSafety reprezintă o responsabilitate trans-curriculară, toate cadrele didactice ar trebui să beneficieze de formare periodică pe teme cum ar fi: confidenţialitatea şi securitatea, amprenta digitală şi reputaţia, cyberbullying-ul, alfabetizarea informaţională etc.
- În predarea acestora şi altor probleme eSafety încercaţi să porniţi de la ceea ce elevii ştiu deja şi de la felul în care experimentează ei mediul online.
- Încurajaţi elevii să se implice în mentorat la egal la egal şi facilitaţi discuţii interactive de jos în sus.

INFORMAŢII PENTRU PĂRINŢI

Părinţii joacă un rol vital în siguranţa online a copiilor şi tinerilor. Desigur, şcolile sunt în măsură să adopte multe măsuri, pot filtra, monitoriza şi educa, dar trebuie să recunoaştem că mulţi copii şi tineri vor avea acasă sau prin intermediul unui dispozitiv mobil un nivel foarte diferit de acces la Internet decât la şcoală. Mulţi părinţi sunt destul de eficienţi în îngrijirea şi îndrumarea copiilor cu privire la problemele offline, dar sunt reticenţi în încercarea de a le oferi sprijin similar în ceea ce priveşte aspectele digitale ale vieţii lor. Parţial acest lucru poate fi un rezultat al faptului că mulţi părinţi spun despre copiii lor că "se pricep mai bine la tehnologie" decât ei.

- Şcolile trebuie să ofere sprijin, îndrumare şi consiliere pentru părinţi. Acest lucru poate lua diverse forme, o discuţie specifică pe această temă, pliante despre diferite probleme, legături (link-uri) pe site-ul şcolii sau un articol în buletinul online al şcolii.
- Este important să recunoaştem că de multe ori părinţii care participă la o seară eSafety sunt tocmai părinţii care probabil nu au nevoie să participe! Părinţii interesaţi de ceea ce

fac copiii lor vor fi, de asemenea, mult mai conştienţi cu privire la problemele cu care aceştia se confruntă online şi vor fi dornici să comunice pe aceste teme.

- Şcolile raportează că implicarea părinţilor în problemele eSafety poate fi o provocare şi că aceştia sunt de multe ori reticenţi în a veni la şcoală pentru astfel de evenimente. În acest caz se recomandă implicarea copiilor şi tinerilor în livrarea acestor mesaje, deoarece părinţii sunt mai înclinaţi să vină la un eveniment în care copilul lor participă direct, de exemplu, prin susţinerea unei prezentări. O altă strategie este livrarea mesajelor eSafety în timp ce părinţii sunt deja în şcoală cu alte scopuri.

UTILIZAREA TEHNOLOGIEI ONLINE DE CĂTRE ELEVI ÎN AFARA ŞCOLII

Incidentele online care au loc în afara şcolii vor avea în mod inevitabil un impact în interiorul şcolii. Cele mai frecvente probleme cu care s-ar putea confrunta o şcoală sunt spargerea conturilor, încălcarea confidenţialităţii, sexting, utilizarea excesivă şi cyberbullying-ul. Este important pentru o şcoală să stabilească dacă şi cum doreşte să răspundă la astfel de evenimente.

- Includeţi o declaraţie în Politica şcolii şi în Politica de Utilizare Acceptabilă cu privire la modul în care vor fi gestionate problemele online care au loc în afara şcolii.
- Informaţi foarte bine părinţii şi elevii cu privire la angajamentul şcolii de a se ocupa de aceste tipuri de probleme.
- Organizaţi în cadrul şcolii activităţi de creştere a gradului de conştientizare pentru a informa elevii de posibilele consecinţe ale problemelor online, cum ar fi bullying-ul şi încălcarea confidenţialităţii. Solicitaţi feedback de la elevi pentru a vedea ce tip de sprijin suplimentar eSafety ar trebui să li se ofere în afara programei.
- Desemnaţi un profesor sau consilier pe care elevii îl pot consulta atunci când se confruntă cu probleme online, indiferent dacă acestea au loc la şcoală sau în afara şcolii. Această persoană ar trebui să fie în măsură să ofere sfaturi tehnice de bază (de exemplu, cum pot să-mi protejeze contul de Facebook), precum şi consiliere psihologică (de exemplu, în cazul unui incident de cyberbullying).
- Atunci când este necesar, o şcoală trebuie să contacteze părinţii tuturor elevilor implicaţi într-o problemă şi dacă este cazul să apeleze la ajutor profesionist extern.
- Urmăriţi numărul şi natura rapoartelor şi identificaţi eventualele nevoi specifice din şcoală..

GESTIONAREA INCIDENTELOR

În toate şcolile au loc incidente şi acestea pot apărea în multe domenii diferite - de la un virus sau atac împotriva serverelor şcolii până la incidente de cyberbullying. Din păcate, incidentele nu sunt privite întotdeauna ca o oportunitate de a învăţa.

- Este important să se revizuiască incidentele la şedinţele periodice cu personalul. Rețineți că imediat după incident ar putea exista o rezistenţă firească la revizuirea incidentului din partea membrilor personalului implicat. Lăsaţi să treacă un timp, astfel încât toată lumea să privească incidentele cu detaşare.
- Discutaţi întrebările din lista de control eSafety atunci când revizuiţi un incident.
- Raportaţi incidentul prin intermediul incident handling report. Raportarea incidentelor prin intermediul unui şablon furnizat pe site va conta în acordarea punctelor de acreditare, va rămâne anonimă și ne va ajuta pe toți să învățăm unii de la alții.

CYBERBULLYING

Cyberbullying – denumit uneori şi bullying online; este o problemă foarte complexă. Poate fi definit ca utilizarea tehnologiei şi în special a telefoanelor mobile şi Internetului, pentru a răni în mod deliberat, supăra, hărțui sau a jena o persoană. Acesta poate fi prelungire a intimidării faţă-în-faţă, tehnologia oferind agresorului o altă metodă de hărţuire a victimei, sau fără niciun motiv. Poate avea loc prin intermediul oricărei forme de media, de la mesaje şi imagini ofensatoare trimise de pe telefoane mobile, la postări neplăcute pe bloguri şi pe rețelele de socializare sau e-mailuri şi mesagerie instantanee, până la site-uri dăunătoare create numai cu scopul de a intimida o persoană sau abuz virtual în timpul unui joc multiplayer online. Cyberbullying-ul diferă de alte forme de bullying: poate invada casa şi spaţiul personal al victimei, publicul este potenţial mai numeros, mesajele sau imaginile supărătoare pot fi propagate rapid și există dificultăți în controlarea și/sau eliminarea mesajelor transmise electronic. De asemenea, deoarece nu presupune interacţiune faţă-în-faţă, cyberbullying-ului i se atribuie de obicei un caracter anonim. Acest lucru îi poate determina pe oameni să se implice în activități în care nici n-ar visa să se implice în lumea reală, fie ca autor sau ca un spectator.

- Se adoptă o abordare anti-bullying la nivelul întregii şcoli.
- Comunicaţi în mod clar strategia pentru toți membrii comunității școlare - elevi, cadre didactice, personal adiţional și părinți. Toată lumea ar trebui să fie conştientă de traseele de raportare și de consecințele pentru cei implicați în astfel de comportamente.
- Se revizuiește periodic strategia adoptată, se evaluează succesul acesteia și adaptați-o dacă este necesar.
- Organizaţi sau încurajaţi formări pentru profesori.
- Integraţi în programă conştientizarea cu privire la (cyber) bullying pentru toate categoriile de vârstă. - Organizaţi sesiuni de informare pentru părinți. Aceştia ar putea să nu fie conştienţi de noile instrumente tehnologice şi de modul în care copiii lor le folosesc.

ASPECTE LEGALE ALE PROTECȚIEI DATELOR

Protecția vieții private și a datelor cu caracter personal ale tuturor elevilor și personalului din școală este reglementată de legislația națională din țara dvs. privind protecția datelor. Deși aceste reguli se bazează pe o Directivă Europeană (95/46/EC) există multe diferențe în modul în care țările au transpus acest document în legislația națională. Pentru a ști ce reguli se aplică în țara dumneavoastră consultați site-ul national Data Protection Authority. *(http://ec.europa.eu/justice/data-protection/bodies/)*

În 2012, Comisia Europeană a propus o reformă majoră a Directivei Europene pentru Protecția Datelor. Noile propuneri vor consolida drepturile individuale și vor aborda provocările globalizării și noilor tehnologii. Puteți urmări discuțiile și deciziile referitoare la această nouă propunere pe EC website *(http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm)* și descoperiți ce implicații ar putea avea acest lucru asupra protecției confidențialității și a datelor cu caracter personal în școala dvs.

Școala își poate exercita dreptul de a monitoriza utilizarea sistemelor informatice, inclusiv accesul la Internet și interceptarea de e-mail-uri, în scopul monitorizării respectării Politicii de Utilizare Acceptabilă și Politicii de Securitate a Datelor. În cazul în care se consideră că are loc folosirea neautorizată și/sau necorespunzătoare a sistemului informatic al serviciului sau un comportament inacceptabil sau necorespunzător, școala va invoca procedura sa disciplinară. Dacă școala suspectează că sistemul poate fi folosit în scopuri criminale sau pentru depozitarea ilegală de text, imagini sau sunet, chestiunea va fi adusă în atenția organelor responsabile cu aplicarea legii.

Am citit şi înţeles şi sunt de acord cu respectarea Politicii de Utilizare Acceptabilă a TIC de către personal.

Semnătură: …….... Nume: …… Dată: ……

Acceptat de: ……..……. Nume: …….