



CIRC. N. 100/ST-D-ATA

Torino, 07 gennaio 2014

Agli ALLIEVI, DOCENTI e PERSONALE ATA dell'ISTITUTO

Oggetto: "Regolamento per un uso corretto e consapevole della rete all'interno dell'IIS Primo Levi"

Regolamento per un uso corretto e consapevole della rete

Il curriculum scolastico prevede il regolare utilizzo dei laboratori informatici dove, oltre a svolgere le normali attività tecniche inerenti la specializzazione, gli studenti impareranno a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le tecnologie per l'informazione e la comunicazione (TIC). Internet offre sia agli studenti che agli insegnanti una vasta scelta di risorse e di opportunità di pubblicazione e scambio. Per questo motivo Internet viene utilizzata da sempre più studenti, mediante le connessioni domestiche, non soltanto per le attività scolastiche ma anche e soprattutto per l'intrattenimento e per il tempo libero.

La scuola propone agli studenti e agli insegnanti di utilizzare internet non soltanto per le attività sociali ma anche per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione. Per gli studenti e per gli insegnanti l'accesso ad internet a scuola, nel rispetto delle disposizioni del Ministero dell'Istruzione Università e Ricerca che vietano l'uso in classe di telefoni cellulari e dispositivi elettronici¹, è un privilegio e un diritto.

Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su internet, la scuola ha limitato l'accesso ad internet mediante il filtro per la navigazione dell'Università di Tolosa e le attività svolte in rete vengono monitorate e tracciate nel rispetto delle vigenti normative sulla privacy. Il filtro da solo non è però in grado di eliminare tutti i rischi, anche perché è possibile commettere errori o attività illegali su siti perfettamente leciti e perché gli studenti sono in grado collegarsi ad Internet senza protezione sia da casa che con il proprio cellulare.

Per questo motivo gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari nell'uso di internet e insegnando un uso dei nuovi strumenti di comunicazione accettabile e responsabile.

La presente Politica per l'Uso Accettabile della Rete della scuola, che fornisce le linee guida per il benessere e la sicurezza di tutti gli utenti della rete, è esposta come regolamento nei laboratori e viene consegnata e sottoscritta a studenti e docenti che richiedono l'accesso alla rete wireless.

I genitori possono ottenere una copia del documento relativo all'uso Accettabile e responsabile di Internet e possono, per qualsiasi dubbio, chiedere consiglio e supporto ai docenti.

Principi di buon comportamento in rete

Fra gli utenti dei servizi telematici Internet, si sono sviluppati nel corso del tempo una serie di principi di buon comportamento che vengono identificati con il nome di Netiquette². Con l'avvento del web 2.0 e dei Social Network³, basati sui principi di collaborazione e condivisione diretta degli utenti, internet e i suoi servizi si sono evoluti, dando vita ad un galateo del web 2.0⁴ che prende il nome di Netiquette 2.0.

Questi principi sono le linee guida fondamentali per la sicurezza e il benessere di tutti nella rete, in particolare negli ambienti più usati dagli adolescenti.

¹ Dispositivi elettronici durante attività didattica www.istruzione.it/normativa/2007/allegati/prot30_07.pdf

² Netiquette: <http://it.wikipedia.org/wiki/Netiquette>

³ Social Network: http://it.wikipedia.org/wiki/Rete_sociale

⁴ Web 2.0: http://it.wikipedia.org/wiki/Web_2.0



I.I.S. PRIMO LEVI

ISTITUTO TECNICO SETTORE TECNOLOGICO

Elettronica ed Elettrotecnica - Informatica e Telecomunicazioni

LICEO SCIENTIFICO LICEO SCIENTIFICO opzione Scienze Applicate



Tutti gli utenti della rete dell'Istituto devono rispettare scrupolosamente questi principi, le leggi vigenti in materia di diritto d'autore e tutela della privacy nonché le specifiche norme penali relative al settore informatico e della comunicazione elettronica, oltre ad ogni altra disposizione generale di legge.

Principi Generali

- 1.** Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, devono essere considerati abusi da segnalare solo i contenuti palesemente impropri o illeciti e non tutti quei contenuti con cui semplicemente non si è d'accordo o non piacciono;
- 2.** Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, Netlog, ecc..., bisogna informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche⁵;
- 3.** Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato, scegliendo con cura le amicizie con cui accrescere la propria rete e i gruppi a cui aderire e proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non banale (evitare nomi del proprio cane, gatto, ecc...);
- 4.** Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non bisogna pubblicare su YouTube video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.
- 5.** Bisogna contribuire a rendere il Web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza;
- 6.** Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto (abuso, data, ora, utenti e servizio coinvolti). Tutti i social network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito. Prima di trasformare un incidente o una "bravata" in una denuncia alle autorità competenti avvalersi della modalità di segnalazione che non obbliga le parti in causa a conseguenze penali e giudiziarie che possono durare anni;

Relazioni tra persone di pari livello – (Rapporto 1 a 1)

- 7.** All'interno dei Social Network si instaurano tante relazioni tra singoli utenti, non veicolate o controllate da intermediari, chiamati rapporti di pari livello. E' importante fare attenzione a quali informazioni vengono fornite in questo contesto, evitando di condividere dati personali e di contatto, come numeri di telefono o indirizzi, che nella vita reale non si darebbero a persone che non sono ancora degne di fiducia;
- 8.** Bisogna evitare di scambiare file con utenti di cui non ci si può fidare e in ogni caso, anche quando si conosce l'interlocutore, è necessario verificare sempre l'origine dei file ed effettuare un controllo con un antivirus aggiornato;
- 9.** Se durante una chat, un forum o in una qualsiasi discussione online, l'interlocutore diviene volgare, offensivo o minaccioso, si deve evitare di fomentarlo, ignorandolo e abbandonando la conversazione;
- 10.** Quando si riscontra un comportamento riconducibile ad un illecito durante una conversazione privata, per esempio un tentativo di approccio sessuale nonostante la minore età, stalking o cyberbullismo, l'utente può sfruttare gli appositi sistemi di reportistica degli

⁵ www.tiseiconnesso.it



I.I.S. PRIMO LEVI

ISTITUTO TECNICO SETTORE TECNOLOGICO

Elettronica ed Elettrotecnica - Informatica e Telecomunicazioni

LICEO SCIENTIFICO LICEO SCIENTIFICO opzione Scienze Applicate



abusi del predisposti all'interno del servizio, segnalando tempestivamente il nickname che ha perpetrato l'abuso. In questi casi può essere conveniente abbandonare non soltanto la conversazione ma anche il profilo personale usato fino a quel momento creandosene uno nuovo.

11. Quando si fa uso di sistemi di file-sharing P2P, è importante evitare di scaricare dei file che possono essere considerati illegali e protetti dal diritto d'autore. Bisogna inoltre fare attenzione e non aprire mai dei file sospetti, verificandone la bontà con un antivirus aggiornato; La maggior parte dei programmi P2P contiene spyware e malware, software malevoli in grado di compromettere seriamente la sicurezza del computer che si sta usando. Per motivi di sicurezza della rete l'utilizzo questi sistemi a scuola è vietato.

12. I sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica quindi è necessario preservare la privacy di tutti, cancellando il mittente o i vari destinatari quando si invia un messaggio a più destinatari che non si conoscono tra loro, evitare di inoltrare spam⁶ o catene di sant'Antonio, o perpetrare qualunque tipo di abuso usando i messaggi elettronici;

13. Quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica di sottofondo bisogna essere sicuri di averne il diritto d'uso e di non utilizzare alcun file coperto da copyright;

Contenuti generati dagli utenti – (Rapporto 1 a N)

14. I contenuti pubblicati sulle applicazioni web dei Social Network, hanno diversi livelli di visibilità, per esempio singoli utenti o tutti gli utenti della rete, che devono sempre essere tenuti a mente, dando a ciascun contributo i corretti livelli di privacy. Pertanto, quando si inizia a pubblicare materiale in una community bisogna studiare ed imparare ad utilizzare correttamente le funzioni per l'impostazione dei livelli di privacy;

15. Dal momento che ciò che viene pubblicato su un Social Network è persistente e spesso non è facile da cancellare, bisogna evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato;

16. Quando si contribuisce con del materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto dalla community, evitando di pubblicare materiale inadeguato e che potrebbe risultare fuori contesto: ci sono momenti e luoghi virtuali per parlare di qualsiasi tema nel rispetto dei propri interlocutori;

17. Se si usa un nuovo servizio messo a disposizione dal Social Network, bisogna informarsi su quali sono gli strumenti per segnalare materiale e comportamenti non idonei, e quali sono le modalità corrette per farlo;

18. Se un contenuto viene moderato e non è più visibile online, probabilmente è non idoneo. Modificare linguaggio e controllare se il punto dove lo si è pubblicato è davvero il posto migliore per quello specifico contenuto;

19. Quando si fa uso di etichette per catalogare un contenuto/utente (TAG), bisogna assicurarsi che sia coerente con il contenuto o che indichi la persona corretta; quando il TAG riguarda una persona sarebbe inoltre opportuno contattarla preventivamente per ottenere il consenso a collegare l'identità della persona al contenuto.

La gestione delle relazioni sociali – Communities – (Rapporto N a N)

20. Le relazioni sociali che si sviluppano all'interno di un Social Network sono simili a quelle reali, deve essere gestita la fiducia verso i propri contatti proprio come accade nella realtà. Bisogna aggiungere alla propria rete di amici solo le persone che hanno in vari modi dimostrato di essere affidabili, con cui si è a proprio agio e di cui siamo a conoscenza della reale identità. Inoltre conviene gestire la propria privacy quando si aggiungono persone su cui si hanno dubbi o non si conoscono affatto

⁶ Spam: l'invio di grandi quantità di messaggi indesiderati <http://it.wikipedia.org/wiki/Spam>



I.I.S. PRIMO LEVI

ISTITUTO TECNICO SETTORE TECNOLOGICO

Elettronica ed Elettrotecnica - Informatica e Telecomunicazioni

LICEO SCIENTIFICO LICEO SCIENTIFICO opzione Scienze Applicate



- 21.** Se si instaura un'amicizia virtuale con persone di cui non si conosce la reale identità, bisogna evitare di condividere contatti e dati personali e contenuti privati, soprattutto se riguardano terze persone;
- 22.** La rete sociale non è facile da controllare quindi bisogna tenere sempre a mente che gli "amici degli amici" o di componenti del proprio "network" sono molti e spesso hanno modo, nonostante siano sconosciuti, di avere accesso alle informazioni e ai contenuti personali;
- 23.** Se si ha accesso alle comunicazioni private di altri utenti, per esempio perché l'utente ha impostato in maniera sbagliata i livelli di privacy, bisogna notificarlo all'utente ed evitare di leggere i messaggi privati;
- 24.** La reputazione digitale è persistente e si diffonde velocemente pertanto non bisogna mai diffamare altre persone, soprattutto se le stesse non sono presenti sul Social Network e non possono accorgersi del danno subito;

Reati e violazioni della legge

Al di là delle regole di buona educazione ci sono comportamenti, talvolta solo apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali dalle conseguenze molto serie. Eccone alcuni:

Reati informatici

La legge 547/93 individua e vieta tutta una serie di comportamenti nell'ambito informatico e che sono stati reputati lesivi per gli interessi non solo di singoli privati cittadini ma anche di persone giuridiche, in particolare per le imprese e gli enti pubblici:

- Accesso abusivo ad un sistema informatico e telematico
 - Attività di introduzione in un sistema, a prescindere dal superamento di chiavi "fisiche" o logiche poste a protezione di quest'ultimo. Art. 615 ter cp.
 - Per commettere il reato basta il superamento della barriera di protezione del sistema o accedere e controllare via rete un PC a insaputa del legittimo proprietario, oppure forzare la password di un altro utente e più in generale accedere abusivamente alla posta elettronica, ad un server o ad un sito su cui non siamo autorizzati.
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
 - L'art 615 quinquies punisce "chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri creato, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento".
 - Per commettere questo reato basta, anche solo per scherzo, diffondere un virus attraverso il messenger o la posta elettronica, spiegare ad altre persone come si può fare per proteggere un computer, un software o una console per giochi oppure anche solo controllare a distanza o spegnere un computer via rete.
- Danneggiamento informatico
 - Per danneggiamento informatico si intende un comportamento diretto a cancellare o distruggere o deteriorare sistemi, programmi o dati. L'oggetto del reato, in questo caso, sono i sistemi informatici o telematici, i programmi, i dati o le informazioni altrui. Art. 635 cp.
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
 - Questo particolare reato viene disciplinato dall'art. 615 quater cp e si presenta spesso come complementare rispetto al delitto di frode informatica.
 - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
 - E' considerato reato anche quando l'informazione viene fraudolentemente carpita con "inganni" verbali e quando si prende conoscenza diretta di documenti cartacei ove tali dati sono stati riportati o osservando e memorizzando la "digitazione" di tali codici.



I.I.S. PRIMO LEVI

ISTITUTO TECNICO SETTORE TECNOLOGICO

Elettronica ed Elettrotecnica - Informatica e Telecomunicazioni

LICEO SCIENTIFICO LICEO SCIENTIFICO opzione Scienze Applicate



- Si commette questo reato quando si carpiscono, anche solo per scherzo, i codici di accesso alla posta elettronica, al messenger o al profilo di amici e compagni.
- Frode informatica
 - Questo delitto discende da quello di truffa e viene identificato come soggetto del reato "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno". Art. 640 ter cp.
 - Il profitto può anche "non avere carattere economico, potendo consistere anche nel soddisfacimento di qualsiasi interesse, sia pure soltanto psicologico o morale".
 - Il delitto di frode informatica molto sovente viene a manifestarsi unitamente ad altri delitti informatici, quali l'Accesso informatico abusivo e danneggiamento informatico in conseguenza a Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

Reati non informatici

Sono da considerare reati non informatici tutti quei reati o violazioni del codice civile o penale in cui il ricorso alla tecnologia informatica non sia stato un fattore determinante per il compimento dell'atto:

- Ingiuria
 - Chiunque offende l'onore o il decoro di una persona presente commette il reato di ingiuria.
 - Incorre nello stesso reato chi commette il fatto mediante comunicazione telegrafica o telefonica o con scritti, o disegni, diretti alla persona offesa.
- Diffamazione
 - Qualcuno che offende la reputazione di qualcun altro, quando all'interno di una comunicazione con più persone si diffondono notizie o commenti volti a denigrare una persona. Art. 595 cp.
 - Aggravante nel caso in cui l'offesa sia recata con un "mezzo di pubblicità" come l'inserimento, ad esempio, in un sito Web o social network di una informazione o un giudizio su un soggetto.
 - La pubblicazione on-line, dà origine ad un elevatissimo numero di "contatti" di utenti della Rete, generando una incontrollabile e inarrestabile diffusione della notizia.
- Minacce e molestie
 - Il reato di minaccia consiste nell'indirizzare ad una persona scritti o disegni a contenuto intimidatorio per via telematica. Art. 612 cp.
 - Può capitare che alcune minacce vengano diffuse per via telematica anche per finalità illecite ben più gravi: come ad esempio obbligare qualcuno a "fare, tollerare o omettere qualche cosa" (Violenza privata: art. 610 cp.) o per ottenere un ingiusto profitto (Estorsione: art. 629 cp.).
 - Sull'onda di questa tipologia di reati, è utile descrivere anche quello di Molestie e disturbo alle persone, disciplinato dall'art. 660 cp. che si fonda sul contattare, da parte di terzi, per finalità pretestuose, il soggetto i cui dati sono stati "diffusi" per via telematica.
 - Ad esempio la pubblicazione del nominativo e del cellulare di una persona on-line, accompagnato da informazioni non veritiere o ingiuriose: ciò potrebbe indurre altre persone a contattare la persona per le ragioni legate alle informazioni su questa fornite.
- Violazione dei diritti d'autore
 - La legge 159/93 sottolinea all'art. 1 che chiunque abusivamente riproduce a fini di lucro, con qualsiasi procedimento, la composizione grafica di opere o parti di opere letterarie, drammatiche, scientifiche, didattiche e musicali, che siano



I.I.S. PRIMO LEVI

ISTITUTO TECNICO SETTORE TECNOLOGICO

Elettronica ed Elettrotecnica - Informatica e Telecomunicazioni

LICEO SCIENTIFICO LICEO SCIENTIFICO opzione Scienze Applicate



protette dalla legge 22 aprile 1941, n. 633 e successive modificazioni, ovvero, pone in commercio, detiene per la vendita o introduce a fini di lucro le copie viola i diritti d'autore.

- o Un primo caso di violazione del diritto d'autore si può verificare quando una copia non autorizzata di un'opera digitale è caricata su un server e messa a disposizione degli utenti. In questo caso, colui che riproduce e fornisce l'opera senza l'autorizzazione da parte del suo autore è considerato soggetto responsabile. Per commettere questo reato basta pubblicare su YouTube un video con una qualsiasi musica di sottofondo senza le dovute autorizzazioni.
- o Un ulteriore possibile violazione del diritto d'autore si verifica quando l'utente ottiene il documento, il software o il brano mp3 messo a disposizione in rete o acquistato e ne fa un uso illegittimo, come ad esempio, rivenderlo a terzi o distribuirlo sulla Rete facendone più copie non autorizzate.
- o La legge italiana sul diritto d'autore consente all'utilizzatore di un software o di un opera multimediale o musicale di effettuare un'unica copia di sicurezza ad uso personale, utile nei casi di malfunzionamento del programma, smarrimento della copia originale etc. Tale copia, salvo autorizzazione della casa di produzione, non può essere ceduta ad altre persone.
- o La duplicazione abusiva (senza autorizzazione) è sanzionata penalmente e colpisce ugualmente anche chi duplica abusivamente non a scopo di lucro, bensì per un semplice fine di risparmio personale.

IL DIRIGENTE SCOLASTICO
Prof.ssa Anna Rosaria TOMA