Protetto: Politica per l'Uso Accettabile della rete della scuola

Politica per l'Uso Accettabile della rete della scuola

Destinatari: Personale scolastico - Studenti

Premessa e finalità

Il curriculum scolastico prevede il regolare utilizzo dei laboratori informatici dove, oltre a svolgere le normali attività tecniche, 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 elettronici, è un privilegio e un diritto.

Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su internet, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online, di stabilire obiettivi chiari nell'uso di internet e insegnare un uso dei nuovi strumenti di comunicazione accettabile e responsabile.

La presente **Politica per l'Uso Accettabile della rete della scuola** si prefigge di fornire le linee guida per il benessere e la sicurezza di tutti gli utenti della rete .

CAPITOLO 1 – Comportamenti

Comportamento in rete e uso consapevole delle Tecnologie

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 Netiquette. Con l'avvento del web 2.0 e dei Social Network, basati sui principi di collaborazione e condivisione diretta degli utenti, internet e i suoi servizi si sono evoluti, dando vita ad un galateo del web2.0 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 dai preadolescenti e dagli adolescenti. 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, vanno considerati abusi meritevoli di segnalazione 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, etc..., 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 tematiche.
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.

Comportamenti nelle relazioni tra persone di pari livello – (Rapporto 1 a 1)

1. 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.
2. 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.
3. 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.
4. 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 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.

5. 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.
6. 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 spam o catene di sant'Antonio, o perpetrare qualunque tipo di abuso usando i messaggi elettronici.
7. 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.

Creazione e diffusione di contenuti generati dagli utenti – (Rapporto 1 a N)

1. 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.
2. 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.
3. 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 della 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.
4. 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.
5. 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.
6. 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.

Gestione delle relazioni sociali – *Communities* – (Rapporto N a N)

1. 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 dubbio non si conoscono affatto.
2. 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.

3. 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.
4. 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.
5. 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.

CAPITOLO 2 – Sicurezza e Uso delle TIC

Rete di Istituto, servizi e postazioni informatiche

Sicurezza nell’uso delle TIC nei Laboratori e nelle Postazioni per Docenti e Studenti

Al fine di garantire una gestione il più possibile corretta, la scuola attua le seguenti strategie:

- il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l’accesso e l’uso della rete interna ed esterna (Internet) secondo i normali canali di protezione presenti nei sistemi operativi e utilizzando, se necessario, software/hardware aggiuntivi come *Firewall*;
- si attrezza per evitare comportamenti che non rientrano nelle norme che il collegio dei docenti delinea in proposito come:
 - scaricare file video-musicali protetti da copyright;
 - visitare siti non necessari ad una normale attività didattica;
 - alterare i parametri di protezione dei computer in uso;
 - utilizzare la rete per interessi privati e personali che esulano dalla didattica;
 - non rispettare le leggi sui diritti d’autore;
 - navigare su siti non accettati dalla protezione interna alla scuola.

Disposizioni, comportamenti, procedure:

- Il sistema informatico è periodicamente controllato dai responsabili;
- la scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina;
- la scuola archivia i tracciati del traffico Internet (log del software proxy principale);
- è vietato scaricare da Internet software non autorizzati;
- al termine di ogni collegamento la connessione deve essere chiusa;
- le verifiche antivirus vengono condotte periodicamente sulle unità di memorizzazione di rete (NAS);
- l’utilizzo di CD, chiavi USB e floppy personali deve essere autorizzato dal docente e solo dopo controllo antivirus;
- la scuola si riserva di limitare il numero di siti visitabili e le operazioni di download;
- il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all’Istituto, sempre nell’ambito del presente regolamento e nel rispetto delle leggi.

Accertamento dei rischi e valutazione dei contenuti di Internet

Nonostante l'attenzione da parte del docente, quando gli alunni accedono ad internet, non si può escludere che lo studente, durante la navigazione sui computer dell'Istituto, si imbatta in materiale non appropriato e/o indesiderato. La scuola non può farsi carico *in toto* delle responsabilità per il materiale non idoneo trovato o per eventuali conseguenze causate dall'accesso al Web. Gli utilizzatori devono quindi essere pienamente coscienti degli eventuali rischi cui si espongono collegandosi alla rete, riconoscendo ed evitando gli aspetti negativi, quali la pornografia, la violenza, il razzismo e lo sfruttamento dei minori.

Utilizzo dei servizi Internet

- L'insegnante di classe, che ha nella propria programmazione l'utilizzo di Internet, è responsabile di quanto avviene nelle proprie ore di laboratorio;
- è vietato utilizzare e-mail personali ad uso privato durante le ore di lezione;
- è vietato l'utilizzo delle postazioni durante le ore di lezione per motivi non strettamente legati alla pratica didattica;
- è permessa la partecipazione a forum nell'ambito dei siti ammessi;
- gli allievi non possono usare i computer dell'Istituto in rete internet senza l'ausilio e il coordinamento del docente; il mancato rispetto da parte degli allievi delle norme definite comporterà un giudizio negativo secondo la normale prassi didattica di valutazione relativa alla condotta e al profitto;
- è vietato il download a fini personali di file musicali, foto, software, video, ecc., tranne nel caso di specifiche attività didattiche preventivamente programmate.

Sicurezza della rete interna (LAN)

L'Istituto dispone di un dominio su rete locale cui accedono i computer dell'amministrazione; le postazioni non legate all'amministrazione non hanno accesso al dominio di Istituto.

La rete interna è protetta da *Firewall* per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati.

La memorizzazione dei documenti è garantita attraverso l'uso di dispositivi di *storage* di rete (NAS) per tutte le postazioni legate alla didattica (laboratori, sale insegnanti, postazioni per studenti e docenti). Su questi dispositivi non è garantito alcun servizio di backup, pertanto si consiglia di fare copia su un supporto personale (pendrive, cd o altro) dei propri dati.

Per quanto concerne la rete amministrativa, lo *storage* è garantito da un apposito server che offre anche servizio di *mirroring* e di *backup* automatico su dispositivo rimovibile.

Sicurezza della rete senza fili (Wireless – WiFi)

L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolato da un server specifico con funzione di captive portal che determina l'accesso degli utenti dietro richiesta di credenziali (nome utente e password).

L'ottenimento delle credenziali è riservato a studenti e personale dell'Istituto, previa richiesta dietro compilazione di apposito modulo, da richiedere all'Amministratore di Rete. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

Linee guida di utilizzo delle TIC per Studenti e Docenti

Studenti

- Non utilizzate giochi né in locale, né in rete;
- salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione di rete (NAS) e non sul desktop o in altre posizioni in locale: le postazioni dedicate alla didattica eliminano qualunque dato alla fine della sessione di lavoro, per ragioni di tutela e sicurezza;
- mantenete segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della vostra scuola;
- non inviate a nessuno fotografie vostre o di vostri amici;
- chiedete sempre al vostro insegnante o ad un adulto il permesso di scaricare documenti da Internet;
- non caricate o copiate materiale da Internet senza il permesso del vostro insegnante o del responsabile di laboratorio.

Docenti

- Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato;
- salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione di rete (NAS) e non sul desktop o in altre posizioni in locale: le postazioni dedicate alla didattica eliminano qualunque dato alla fine della sessione di lavoro, per ragioni di tutela e sicurezza;
- discutete con gli alunni della PUA della scuola e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate;
- ricordate di verificare lo stato dei computer alla fine della sessione di lavoro, in particolare controllando che siano tutti spenti all'uscita dall'ora di lezione nei laboratori e dall'ultima ora di lezione nelle classi in cui è presente una L.I.M.;
- ricordate agli alunni che la violazione consapevole della PUA della scuola comporta la temporanea sospensione dell'accesso ad Internet per un periodo commisurato alla gravità del fatto. La violazione o il dolo accertati, oltre all'intervento disciplinare del consiglio di classe, daranno luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile; rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni, nonché l'eventuale denuncia del reato all'autorità giudiziaria. Nel caso di infrazione consapevole da parte dei docenti sarà compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti.

Sito web dell'Istituto

L'Istituto dispone di un proprio spazio web e di un proprio dominio:
<https://www.iismorellicolao.edu.it/>

L'Istituto gestisce un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Webmaster. La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.

La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

CAPITOLO 3 – Informazione

Informazione sulla Politica d'Uso Accettabile delle TIC della scuola

Informazione del personale scolastico

Tutto il personale scolastico (docente ed ATA) analizzerà la Politica d'Uso Accettabile delle TIC sottoscrivendola all'inizio dell'anno scolastico, all'inizio del rapporto di lavoro ed ogni qualvolta vi sarà apportata una variazione e sarà coinvolto nel suo ulteriore sviluppo, sempre tenendo conto che l'uso della rete sarà sottoposto a monitoraggio.

Informazione degli alunni

Sarà cura del docente responsabile del laboratorio e dei vari docenti utenti del medesimo illustrare didatticamente i contenuti della Politica d'Uso Accettabile delle TIC agli allievi, tenendo conto della loro età ed evidenziando le opportunità ed i rischi connessi all'uso della comunicazione tecnologica.

Informazione dei genitori/tutori

I genitori saranno informati sulla politica d'uso accettabile e responsabile di Internet nella scuola e sulle regole da seguire a casa tramite:

- esposizione del seguente documento all'albo;
- pubblicazione dello stesso sul sito web della scuola.

CAPITOLO 4 – Disposizioni di legge e sanzioni

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. Alcuni esempi:

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:

- DANNEGGIAMENTO INFORMATICO
- DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI
- FRODE INFORMATICA

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
- DIFFAMAZIONE
- MINACCE E MOLESTIE
- VIOLAZIONE DEI DIRITTI D'AUTORE

Sanzioni

A fronte di violazioni delle regole stabilite dalla politica scolastica, la scuola, su valutazione del responsabile di laboratorio e del Dirigente Scolastico, si assume il diritto di impedire l'accesso dell'utente a Internet per un certo periodo di tempo, rapportato alla gravità.

La violazione o il dolo accertati, oltre all'intervento disciplinare del consiglio di classe, daranno luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile; rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni, nonché l'eventuale denuncia del reato all'autorità giudiziaria.

Nel caso di infrazione consapevole da parte dei docenti o del personale non docente si interverrà per via amministrativa secondo le norme vigenti.

Materiale utile scaricabile, del Garante per la privacy disponibile sul sito <http://www.garanteprivacy.it/socialprivacy>