ISTITUTO DI ISTRUZIONE SUPERIORE STATALE
"James Clerk MAXWELL"
via Don G. Calabria, 2 - 20132 Milano tel. 02282.5958/6328 Fax 022841996 – www.maxwell.mi.it

SEZIONE ASSOCIATA I. P. S. I. A. *"Luigi SETTEMBRINI"*
via Narni, 18 - 20132 Milano tel. 022614.3954/5080 Fax 022871730 – www.settembrini.mi.it

C. F. 80124170152

Politica per l'Uso Accettabile della Rete

Il Dirigente Scolastico,
preso atto delle seguenti leggi di riferimento:

- L. 135/2012, del 07/08/2012, "Conversione in legge, con modificazioni, del decreto–legge 6/07/2012, n. 95, recante disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini";
- L. 633/1941, Testo consolidato al 09/02/2008, "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio";
- D.Lgs. 305/2006 del 07/12/2006, "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione", in attuazione degli articoli 20 e 21 del D.Lgs. 30/06/2003, n. 196, "Codice in materia di protezione dei dati personali";
- L. 4/2004, "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici";
- D.Lgs 196/2003 Testo Unico sulla privacy entrato in vigore il 01/01/2004 che riassume le norme precedenti sulla privacy;
- D.Lgs 68/2003, "Sulla regolamentazione per la tutela del diritto d'autore e dei diritti connessi nella società dell'informazione";
- C.M. 114/2002, "Sulle infrastrutture tecnologiche nelle scuole e nuove modalità di accesso al sistema informativo";
- C.M. 152/2001, "Sulla diffusione delle reti LAN";
- L. 325/2000, "Sull'adozione delle misure di sicurezza nel trattamento dei dati in applicazione dell'art.15 della Legge 675/1996";
- L. 248/2000, "Nuove norme di tutela del diritto d'autore";
- D.P.R. n. 275 del 25/02/1999, "Regolamento recante norme in materia di autonomia delle istituzioni scolastiche", ai sensi dell'art. 21 della legge 15/03/1997, n. 5;
- L. 547/1993, "Norme in materia di reati informatici".

Visti inoltre i seguenti documenti:

- Il comunicato stampa del Garante per la protezione dei dati personali, "La privacy a scuola. Dai tablet alla pagella elettronica. Le regole da ricordare", del 06/09/2012;
- Il "Regolamento Interno" della Scuola approvato in Consiglio d'Istituto;
- La "Nota informativa sul trattamento dei dati personali", ai sensi della L. 675/96 e s.m. e i. ("Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") che è parte integrante del regolamento interno sottoscritto dai genitori o da chi ne fa le veci all'atto della consegna del libretto delle comunicazioni scuola-famiglia della Scuola;
- Le "Linee guida per i siti web della PA", del 26/07/2010;

emana

il documento "Politica d'uso accettabile e sicuro della rete e Regolamento di accesso e utilizzo delle risorse tecnologiche". Questo documento è stato discusso e approvato nel Collegio Docenti del 10 febbraio 2015 e nel Consiglio di Istituto del medesimo giorno; pertanto verrà indicato nel POF, revisionato annualmente e le eventuali revisioni saranno sottoposte all'approvazione degli Organi Collegiali competenti.

Premessa

È ormai normale che a scuola ci si connetta al vasto mondo di Internet sia per svolgere significative esperienze formative, sia per condurre in modo più efficiente le funzioni amministrative. Via Internet si può facilmente fare ricerca, comunicare, documentare i propri elaborati attraverso la pubblicazione dei lavori realizzati in classe mettendo in comune tali esperienze nel Web. Altrettanto facilmente la Pubblica Amministrazione interconnette i suoi Uffici centrali e periferici attraverso la rete. Nello stesso tempo non si può ignorare che Internet è anche una potenziale fonte di rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usarla e alla consapevolezza delle funzioni che la Rete rende possibili. Stesso discorso deve oggi essere fatto per il complesso sistema di computer in rete presenti nella scuola, sia riguardo ai tradizionali laboratori, sia riguardo agli uffici amministrativi e più in generale alle aule singole o specifiche predisposte per il collegamento interno ed esterno. Le linee guida riportate di seguito intendono dare nel nostro Istituto un impulso allo sviluppo di una cultura d'uso corretto e consapevole di Internet, sia tramite il richiamo a norme vigenti, sia con l'indicazione di prassi opportune per un uso sempre più professionale da parte di tutto il personale. Il documento è parte integrante del Regolamento di Istituto e sarà portato a conoscenza dei genitori, degli allievi e di tutto il personale della scuola e da loro sottoscritto; con questo atto si vuole attivare e mantenere nella nostra scuola una "Politica di uso accettabile" (PUA) in materia di "Tecnologie dell'Informazione e della Comunicazione" (TIC) da tutti accettata. Il regolamento non va riferito solo ai pericoli presenti in Internet, ma anche alla rete interna dell'Istituto, il cui uso improprio può generare problemi da un punto di vista didattico, difficoltà di uso delle macchine, fino al blocco delle stesse, comportando un danno funzionale ed anche economico. Inoltre, poiché non è sempre chiaro quali siano le responsabilità in caso di conseguenze civili e penali, che comunque esistono, derivanti dall'uso improprio delle TIC, è importante e prioritario definire all'interno dell'istituzione scolastica delle regole chiare che pongano le basi per lavorare serenamente, sicuri di aver messo in atto quanto possibile in chiave di prevenzione, ma soprattutto per usare in modo efficiente e didatticamente costruttivo le suddette tecnologie. Nel documento che definisce la PUA d'Istituto sono definiti ordinamenti in merito a:

- accesso alle postazioni in rete della scuola dei diversi soggetti operanti nell'Istituto: personale in servizio, allievi, eventuali soggetti esterni alla scuola;
- accesso ai servizi resi disponibili sui computer in rete dei diversi soggetti operanti nell'Istituto;
- garanzie a tutela della privacy nell'uso degli strumenti tecnologici d'Istituto.

Vengono inoltre predisposti strumenti hardware e/o software da impiegare per evitare o ridurre al minimo:

- l'uso improprio dell'accesso a Internet, in particolare riguardo alla gestione relativa al traffico generato sulla LAN in uscita e in entrata verso Internet;
- i danni causati da virus o da software che viola le norme sopra definite;
- il rischio di intrusioni indesiderate dall'esterno della LAN;
- i tempi di recupero della piena funzionalità dell'infrastruttura.

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 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 o altrove video girati di nascosto e dove sono presenti persone filmate senza il loro consenso, indipendentemente dal mezzo utilizzato per la registrazione o ripresa.
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 effettuarne 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 le cosiddette 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.

<u>Creazione e diffusione di contenuti generati dagli utenti – (Rapporto 1 a N)</u>

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.

<u>Gestione delle relazioni sociali – Communities – (Rapporto N a N)</u>

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 dubbi o 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.

Sicurezza e Uso delle TIC

Rete di Istituto, servizi e postazioni informatiche

Sicurezza nell'uso delle TIC nei Laboratori e nelle Postazioni per Docenti, Personale ATA 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 che verranno designati di anno in anno, 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; inoltre chiede ai responsabili di vigilare perché siano garantiti i diritti alla privacy, come da normativa vigente;
- 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;
- le postazioni pc in ambiente Windows sono protette da software che impedisce modifiche ai dati memorizzati sul disco fisso interno;
- al termine di ogni collegamento la connessione deve essere chiusa;
- verifiche antivirus vengono condotte periodicamente sui computer e sulle unità di memorizzazione di rete;
- l'utilizzo di CD, chiavi USB e floppy personali deve essere autorizzato dal docente e solo previa scansione antivirus per evitare qualsiasi tipo di infezione alla rete d'Istituto;
- 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

Il sistema di accesso ad Internet della scuola prevede l'uso di un filtro sui contenuti per evitare l'accesso a siti web con contenuto illegale, violento, pedo-pornografico, razzista o comunque non conforme alla policy adottata. In particolare il sistema tende a:

- impedire l'accesso a siti non appropriati;
- monitorare e tracciare i collegamenti di ogni utente;
- regolamentare l'utilizzo di risorse online quali chat, mail e forum.

Nonostante tali mezzi di prevenzione 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 dispositivi informatici dell'Istituto o personali, nella 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, tali postazioni sono su una rete locale isolata dal resto della rete di Istituto. Il collegamento di computer portatili o palmari personali alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico; è prevista la fornitura del servizio DHCP per l'assegnazione automatica di un indirizzo di rete.
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 e delle impostazioni personali è garantita attraverso le funzionalità di Google Drive, che archivia nel cloud messo a disposizione dell'Istituto da parte di Google i dati, e li rende disponibili in tutte le postazioni legate alla didattica (laboratori, sale insegnanti, postazioni per studenti, docenti) e all'area amministrativa (personale ATA). Su questi dispositivi e/o postazioni 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, è garantito un servizio di backup automatico su NAS per le informazioni memorizzate sui server.

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 che determina l'accesso degli utenti dietro richiesta di credenziali (nome utente e password).
L'ottenimento delle credenziali è riservato a studenti, docenti e personale ATA dell'Istituto, mediante sottoscrizione di apposito modulo/dichiarazione, da richiedere al Dirigente Scolastico. Le regole di comportamento sono analoghe a quelle per la connessione alla rete cablata di Istituto.

Linee guida di utilizzo delle TIC per Studenti, Docenti e Personale ATA

Studenti

- Non utilizzate giochi né in locale, né in rete;
- non effettuate riprese video e/o fotografie con alcuno strumento, personale o scolastico, se non con motivazione didattica e su esplicito invito del docente;
- salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione esterni e non in posizioni sull'hard disk 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 al personale tecnico il permesso di scaricare documenti da Internet;
- chiedete sempre il permesso prima di iscrivervi a qualche concorso o prima di riferire l'indirizzo della vostra scuola;
- riferite al vostro insegnante se qualcuno vi invia immagini e/o foto che vi infastidiscono e non rispondete; riferite anche al vostro insegnante se vi capita di trovare immagini di questo tipo su Internet;
- se qualcuno su Internet vi chiede un incontro di persona, riferitelo al vostro insegnante, comunque ad un adulto;
- ricordatevi che le persone che incontrate nella rete sono degli estranei e non sempre sono quello che dicono di essere;
- non è consigliabile inviare mail personali, perciò rivolgetevi sempre al vostro insegnante prima di inviare messaggi di classe;
- 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;
- non effettuate riprese video e/o fotografie e/o audio con alcuno strumento, personale o scolastico, se non con motivazione didattica e avendo informato il dirigente scolastico;
- salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione esterni e non sull'hard disk 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'ultima ora di lezione;
- 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.

Personale ATA

- Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola;
- salvate sempre i vostri lavori (file) in cartelle personali o su dispositivi di memorizzazione esterni e non sull'hard disk locale: le postazioni dedicate alla didattica eliminano qualunque dato alla fine della sessione di lavoro, per ragioni di tutela e sicurezza;
- ricordate di verificare lo stato del computer alla fine della sessione di lavoro, in particolare controllando che sia spento al termine della giornata lavorativa;
- ricordate 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, 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 del personale ATA 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 www.maxwell.mi.it per la sede principale e un proprio spazio web e relativo dominio www.settembrini.mi.it per la sezione associata.
L'Istituto gestisce il proprio sito web in uno spazio di proprietà mentre gestisce il sito web della sezione associata in uno spazio messo a disposizione dal provider. La gestione dei due siti web della scuola e della sezione associata, la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione sono a cura dei rispettivi Webmaster. La scuola detiene i diritti d'autore dei documenti che si trovano sui propri siti o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sui siti della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.
La scuola, in qualità di ente pubblico, pubblicherà sui propri siti 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.

Informazione sulla Politica d'Uso Accettabile delle TIC della scuola

Informazione del personale scolastico

Le regole di base relative all'accesso ad Internet, parte integrante del regolamento d'Istituto, sono pubblicate sul sito, esposte all'albo dell'Istituto, all'interno dei laboratori di informatica e negli uffici amministrativi.
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.

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:

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 eliminare le protezioni di 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, 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 carpita in modo fraudolento 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.
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 online, 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 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.
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.
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.
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.
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.

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 sarà compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti.

Glossario

Black list: regole di filtraggio per il firewall
Credenziali: user name – password: sono personali ed incedibili
Firewall: filtra tutti i pacchetti (dati) in entrata ed in uscita secondo regole prestabilite (black list)
LIM (L.I.M.): Lavagna Interattiva Multimediale
Navigazione: Operazione di ricerca di informazioni su Internet attraverso il Web.
Online: essere connesso ad una rete informatica; contenuti disponibile e fruibili su internet
PUA: Politica d'Uso Accettabile delle TIC
Rete: PC collegati in maniera tale da permettere lo scambio e/o la condivisione di dati
TIC: Tecnologie dell'Informazione e della Comunicazione nella scuola
Web: World Wide Web (www)
Wi-fi: tecnologia che consente a terminali di utenza di collegarsi tra loro attraverso una rete locale in maniera wireless (wlan), ossia senza l'uso di cavi.
Webmaster (o Web master): termine inglese usato anche nella lingua italiana, indica generalmente colui che progetta (webdesigner), costruisce (webdeveloper), amministra/gestisce un sito web e cura il posizionamento, studia il mercato e sviluppa i rapporti tramite il web

IL DIRIGENTE SCOLASTICO
(Prof. Franco Tornaghi)