Regolamento per l'utilizzo di Internet e della rete informatica all'interno dell'istituto (L. n. 35/2012 art. 34)

Art. 1 - Premessa

Il presente Regolamento, parte integrante del Regolamento di istituto del ITET "G.Tomasi di Lampedusa" di S.Agata di Militello, si applica alle modalità di utilizzo della rete LAN (Local Area Network) per la didattica e i servizi amministrativi e di Internet.
L'accesso alla rete web a scuola deve essere effettuato nel rispetto di quanto riportato nelle disposizioni del Ministero dell'Istruzione Università e Ricerca.
Poiché esiste la possibilità che gli alunni trovino materiale inadeguato e/o illegale su internet, la scuola ha limitato l'accesso alla rete mediante un sistema di protezione e di sicurezza informatica (Firewall) che permette di filtrare ciò che arriva attraverso Internet e di limitare gli utilizzi della rete, vietando la connessione a siti ritenuti non affidabili o pericolosi.
Per l'attività amministrativa sono state adottate le misure minime, secondo quanto previsto dal D. P.R. 318/99 : password, codice identificativo personale per ogni utente; programmi antivirus; protezione con firewall e regolamentazione degli accessi ai locali che ospitano i dati riservati o in cui si trovano le postazioni di lavoro; criteri per garantire integrità e trasmissione sicura dei dati.
Con l'avvento e la diffusione dei social network, Internet e i suoi servizi si sono evoluti dando vita ad un galateo del web 2.0 al quale tutti i netizen (cittadini della rete) devono fare riferimento per la sicurezza e il benessere nella rete.
Tutti gli utenti della rete del Scuola sono tenuti a rispettare le leggi vigenti in materia di diritto d'autore e tutela della privacy, nonché le specifiche norme penali relative al settore informatico e alla comunicazione elettronica, oltre ad ogni altra disposizione generale di legge.

Art.2 - I principi fondamentali di Internet

I principi fondanti della rete si possono dividere in cinque sezioni, che identificano gli ambiti a cui tali principi afferiscono:

a) principi generali, che definiscono le caratteristiche principali dell'infrastruttura

b) cittadinanza in rete
c) utenti in quanto consumatori di servizi in Internet
d) produzione e circolazione dei contenuti
e) sicurezza in rete.

Art.3 – Relazioni tra cittadini digitali

Ecco le regole da rispettare:

a) occorre contribuire a rendere il web un luogo sicuro, pertanto ogni volta che un utente commette un abuso o un errore pubblicando materiale illecito, non idoneo o offensivo, occorre contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza;
b) ogni abuso subito o rilevato nella navigazione deve essere segnalato tramite gli strumenti offerti dal servizio per ottenere la rimozione del contenuto. Prima di trasformare un incidente o una bravata in una denuncia alle Autorità competenti vale la pena di segnalare il fatto ai gestori del relativo sito per non incorrere in conseguenze penali e giudiziarie;
c) se si condividono informazioni personali, prima della pubblicazione occorre scegliere con cura cosa rendere pubblico e cosa mantenere privato, scegliere con attenzione le amicizie con cui accrescere la propria rete e proteggere la propria identità digitale con password;
d) 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 si devono pubblicare video girati di nascosto e dove sono presenti persone filmate senza il loro consenso;
e) bisogna evitare di scambiare file con utenti di cui non ci si può fidare, in ogni caso anche quando si conosce l'interlocutore, è necessario verificare sempre l'origine del file ed effettuare un controllo con un antivirus aggiornato;
f) se durante una conversazione online l'interlocutore diviene volgare, offensivo o minaccioso si deve abbandonare la conversazione;
g) nell'uso di sistemi di file-sharing P2P (Peer-to-peer), evitare di scaricare dei file che possono essere considerati illegali e/o protetti dal diritto d'autore, non aprire mai dei file sospetti (la maggior parte dei programmi P2P contiene spyware e malware).Per motivi di sicurezza la scuola vieta l'utilizzo di questi sistemi;
h) i sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica quindi, quando si invia un messaggio a più destinatari che non si conoscono tra loro, è necessario evitare che i

destinatari possano vedere e conoscere i propri indirizzi di posta elettronica;

i) 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 files coperti da copyright;
j) i contenuti pubblicati sulle applicazioni web dei Social Network hanno diversi livelli di visibilità (es. singoli utenti o tutti gli utenti delle rete) che devono essere tenuti a mente dando a ciascun contributo i corretti livelli di privacy;
k) quando si contribuisce a pubblicare materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto, evitando di pubblicare materiale inadeguato: ci sono luoghi virtuali per parlare di qualsiasi tema nel rispetto dei propri interlocutori.
l) la reputazione digitale si diffonde velocemente, pertanto non si devono diffamare altre persone, soprattutto se le stesse non sono presenti sul Social network e non possono accorgersi del danno subito;
m) è possibile la pubblicazione di foto di alunni purchè queste riguardino momenti positivi di vita scolastica, dal momento che con l'informativa sulla privacy, fornita al momento dell'iscrizione, le famiglie sono state informate dell'evenienza.

Art. 4 - Operazioni non autorizzate

a) E' vietato a studenti, docenti e al personale tecnico e amministrativo installare programmi non autorizzati sulle postazioni informatiche della scuola. Qualora fosse necessario, solo ed esclusivamente per fini didattici o amministrativi, installare software non ancora in dotazione alla scuola, la persona direttamente interessata deve produrre apposita richiesta al Dirigente scolastico specificando: tipo di programma, utilizzo, eventuale costo, attività interessate e previste con il programma richiesto.
b) Solo dopo un'accettazione da parte di una commissione costituita dal Dirigente Scolastico, D.S.G.A. e i componenti della Commissione web, si potrà procedere all'acquisto e all'istallazione del software.
c) E' vietata la pubblicazione nel sito della scuola di qualsiasi documento, sia esso didattico o amministrativo, senza che la stessa sia stata autorizzata dal Dirigente Scolastico, che avrà provveduto a vistare il materiale.
d) E' vietata l'installazione di propri programmi; è vietata l'installazione di propri dispositivi senza l'autorizzazione del Dirigente scolastico o senza la preventiva scansione con un valido programma antivirus della scuola.

e) E' vietato modificare i programmi installati nei pc o alterarne le configurazioni agendo su software o hardware.
f) E' vietato accedere ai servizi utilizzando l'account di un altro utente.

Art.5 - Reati e violazioni della legge

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:

a) Accesso abusivo ad un sistema informatico e telematico
    1. 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.
    2. Per commettere il reato basta il superamento della barriera di protezione del sistema
b) 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.
c) Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
    1. 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".
    2. 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 sproteggere un computer, un software o una console per giochi oppure anche solo controllare a distanza o spegnere un computer via rete.
d) Danneggiamento informatico

    1. 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.

e) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

1. Questo particolare reato viene disciplinato dall'art. 615 quater cp e si presenta spesso come complementare rispetto al delitto di frode informatica.
2. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
3. E' considerato reato anche quando l'informazione viene fraudolentamente 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.
4. 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.

f) Frode informatica

1. 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.
2. Il profitto può anche "non avere carattere economico, potendo consistere anche nel soddisfacimento di qualsiasi interesse, sia pure soltanto psicologico o morale".
3. 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:

a) Ingiuria
   1) Chiunque offende l'onore o il decoro di una persona presente commette il reato di ingiuria.
   2) Incorre nello stesso reato chi commette il fatto mediante comunicazione telegrafica o telefonica o con scritti, o disegni, diretti alla persona offesa.

b) Diffamazione
   1) 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.
   2) 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.
   3) La pubblicazione on-line, dà origine ad un elevatissimo numero di "contatti" di utenti della Rete, generando una incontrollabile e inarrestabile diffusione della notizia.

c) Minacce e molestie
   1) Il reato di minaccia consiste nell'indirizzare ad una persona scritti o disegni a contenuto intimidatorio per via telematica. Art. 612 cp.
   2) 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.).
   3) 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).

d) Violazione dei diritti d'autore

   1) 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.

2) 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).
3) 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 (ad esempio: rivenderlo a terzi o distribuirlo sulla Rete facendone più copie non autorizzate).
4) 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.
5) 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.