Ministero dell'Istruzione
dell'Università e della Ricerca

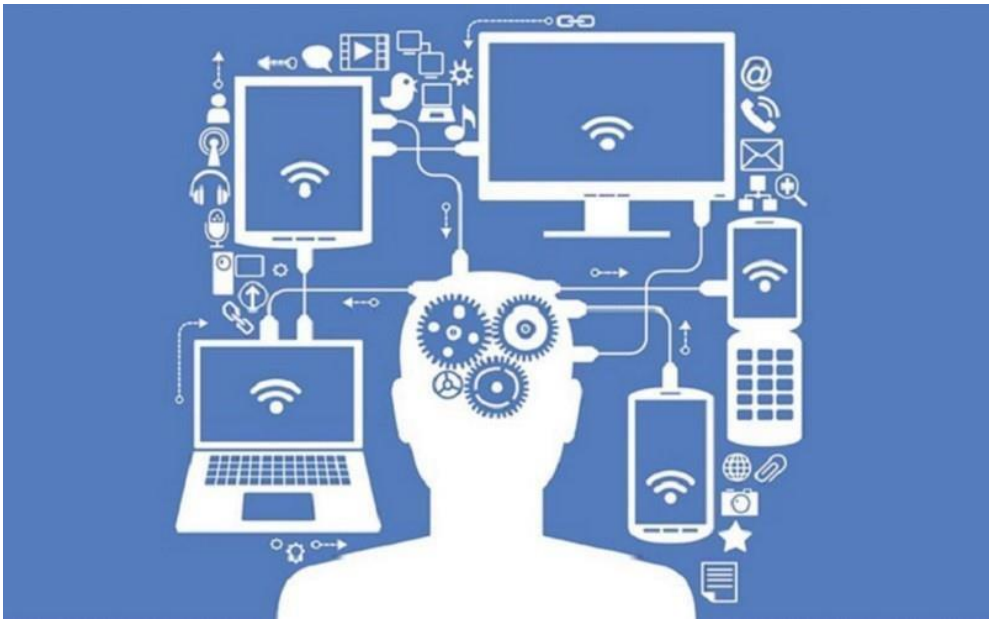
ISTITUTO D'ISTRUZIONE SUPERIORE
"ROCCO SCOTELLARO"

80046 S. GIORGIO A CREMANO (NA) Via Carducci, 31 Tel. 081-7711744-FAX 081- 5746721

REGOLAMENTO P.U.A

POLITICA DI USO ACCETTABILE

SICUREZZA INFORMATICA ED USO CONSAPEVOLE NELLA SCUOLA DELLE T.I.C.



A. S. 2019-2020

Approvato con delibere N. del Consiglio di Istituto del

PREMESSA

Negli ultimi anni la nostra scuola si è dotata di attrezzature informatiche e multimediali di ultima generazione per consentire una modernizzazione delle attività formative, con metodologie e applicazioni di una didattica sostenuta dall'uso delle TIC.

Il curricolo scolastico prevede il regolare utilizzo delle TIC con cui, oltre a svolgere le normali attività tecniche inerenti la specializzazione, gli studenti imparano a trovare materiale, recuperare documenti e scambiare informazioni. Internet offre sia agli studenti che agli insegnanti un'ampia scelta di risorse e di opportunità di pubblicazione e scambio. Per questo motivo Internet viene utilizzato 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 anche per promuovere le eccellenze 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.

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

Il nostro Istituto ha deciso di attivare e mantenere una "Politica di uso accettabile" (PUA) in materia di ''Tecnologie dell'Informazione e della Comunicazione" (TIC), intendendo dare 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 scolastico, con la dovuta competenza a seconda dei diversi gradi di utilizzo.

Tutti gli utenti della rete dell'Istituto devono rispettare scrupolosamente questi principi, le leggi vigenti in mate ria 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 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).

CAPITOLO 1 Comportamenti

Creazione e diffusione di contenuti generati dagli utenti -

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.

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 è inoltre opportuno contattarla preventivamente per ottenere il consenso a collegare l'identità della persona al contenuto.

Gestione delle relazioni sociali – Communities

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.

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 sempre considerare 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

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

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

1. 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;

2. il Dirigente Scolastico si attrezza per evitare comportamenti che non rientrino nelle norme che annualmente 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 MS Windows sono protette da software che impedisce modifiche ai dati memorizzati sul disco rigido interno;
- al termine di ogni collegamento la connessione deve essere chiusa;
- verifiche antivirus vengono condotte periodicamente su eventuali 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;
- 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 macchina;
- ✓ 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. 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 ed 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

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.
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.

Sicurezza della rete senza fili (Wireless – WiFi) e cablata

L'Istituto dispone di una rete con tecnologia senza fili nonché di una rete cablata.
La rete wireless (quando attiva), è protetta da password alfanumerica e l'accesso degli utenti avviene esclusivamente dietro richiesta di password.
L'ottenimento della password è riservato a docenti e personale dell'Istituto, previa richiesta.
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 o su dispositivi di memorizzazione di rete (NAS), se presenti, e non sul desktop o in altre posizioni in locale: le postazioni dedicate alla didattica potranno eliminare 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;
- 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 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; 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; salvate sempre i vostri lavori (file) in cartelle personali o su dispositivi di memorizzazione di rete (NAS), se presenti, e non sul desktop o in altre posizioni in locale: le postazioni dedicate alla didattica potranno eliminare 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 ed affidabile; rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante, 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.
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.

Servizi on line a studenti, famiglie e utenti esterni

La scuola offre all'interno del proprio sito web i seguenti servizi agli studenti, alle famiglie ed agli utenti esterni:

- Informazioni
  - Informazioni generali sull'Istituto
  - Informazioni sull'Offerta Formativa e Orientamento scolastico
  - Informazioni sui Progetti attivati dall'Istituto
  - Informazioni sull'Amministrazione dell'Istituto
  - Albo di Istituto, Avvisi e comunicazioni
- Attività
  - Comunicazione, giornalismo e multimedialità on line
  - Prodotti interattivi realizzati dalle classi
- Strumenti di utilità (da realizzarsi)
  - funzionalità di didattica on line
  - Sezione Intranet: avvisi e comunicazioni
  - Sezione Intranet: modulistica
  - Web Mail di Istituto

Servizi on line per i docenti

La scuola offrirà all'interno del proprio sito web i seguenti servizi e strumenti di lavoro per i docenti:

- Programmazione on line: strumento per la messa in rete dei programmi delle materie;
- strumento di archiviazione ed elaborazione di unità e contenuti didattici;

Altre forme tecnologiche di comunicazione

Agli allievi non è permesso utilizzare i telefoni cellulari per telefonare, scattare foto o registrare filmati durante le lezioni o durante l'orario scolastico. È vietato inviare messaggi illeciti o inappropriati, nonché fotografie o filmati.
Ai docenti ed al personale che entra in diretto contatto con gli allievi, è altresì vietato l'uso del telefono cellulare durante lo svolgimento delle lezioni se non per ragioni di estrema urgenza

CAPITOLO 3 – Informazione

Informazione del personale scolastico

Le regole di base relative all'accesso ad Internet, parte integrante del regolamento d'Istituto, sono 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:

a. esposizione del seguente documento all'albo;
b. pubblicazione dello stesso sul sito web della scuola;
c. consultazione del documento in segreteria.

La scuola, inoltre, all'atto dell'iscrizione, chiede a chi esercita la responsabilità genitoriale sugli studenti, il consenso all'uso di Internet per il loro figlio e per la pubblicazione dei suoi lavori e della sue fotografie per finalità esclusivamente didattiche.

CAPITOLO 4 – Disposizioni di legge e sanzioni

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:

1. **Accesso abusivo ad un sistema informatico e telematico**

Diffusione di programmi diretti a danneggiare o interrompere un sistema

informatico. L'art 615 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.

2. **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.

3. **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.
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 siano 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.

4. **Frode informatica**

Questo reato 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 ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno”. Art. 640 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 siano stati "diffusi" per via telematica

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.
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.