Protocollo e-safety e uso consapevole della rete

Il curricolo scolastico prevede il regolare utilizzo dei laboratori informatici in quanto ambienti formativi atti a svolgere attività didattiche implementate dal digitale, gli studenti possono imparare a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le Tecnologie per l'Informazione e la Comunicazione (ICT).
Data la vastità del materiale reperibile in Rete e l'utilizzo talvolta smodato e inconsapevole degli spazi digitali da parte degli studenti, la scuola propone l'utilizzo di internet non soltanto per le attività sociali, ma anche per incentivare all'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione.
Coerentemente con quanto disposto dal PNSD, è stato normato e regolamentato l'uso dei mezzi informatici nelle scuole, garantendo un utilizzo responsabile dei dispositivi elettronici, al fine di rendere la didattica innovativa, nel contesto di una scuola al passo con una società digitalizzata e avanzata.
L'accesso ai fondi Pon ha permesso alla scuola l'acquisto di un filtro, che limiti o proibisca la navigazione in spazi inadeguati e illegali, e che, associato al firewall, permette il monitoraggio della navigazione nel rispetto di quanto disposto dalla normativa vigente in materia di privacy.
E' compito dell'insegnante guidare gli studenti nelle attività on-line al fine di inferire comportamenti responsabili nell'utilizzo della Rete anche in modalità autonoma, attraverso l'uso del telefonino, tablet in modalità BYOD o dei device in dotazione all'istituto.
La presente Politica per l'Uso Accettabile della rete della scuola, che fornisce le linee guida per il benessere e la sicurezza di tutti gli utenti della rete, viene diffusa all'interno dell'Istituto e resa disponibile sul sito web della scuola.

CAPITOLO 1 - Comportamenti
Comportamento in rete e uso consapevole delle Tecnologie

La diffusione dei mezzi telematici e l'accesso smodato agli innumerevoli servizi offerti dal web, ha fatto nascere fra gli utenti la necessità di condividere un sistema di norme e di buoni comportamenti, noti con il nome di Netiquette. Nell'era digitale del Web 2.0 esse sono parte fondante dei comportamenti attesi, in termini di collaborazione e condivisione diretta fra gli utenti, e costituiscono ciò che si può definire il galateo di comportamento, evoluto in 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, all'interno 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

Considerato Internet come garante della libera espressione e informazione, è importante che l'utente conosca i vincoli posti dal sistema informatico, dove è possibile segnalare i contenuti impropri o illegali ma non manifestare dissensi.
E' dovere quindi dell'utente verificare l'attendibilità, la veridicità e le clausole contrattuali di alcune tipologie di servizi, quali i 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.

La condivisione delle informazioni personali deve essere ponderata, selezionando i contenuti opportuni da rendere pubblici, i contatti e le amicizie virtuali nonchè la partecipazione ai gruppi di interesse. E' altresì importante proteggere la propria identità digitale attraverso l'utilizzo di password complesse e domande di recupero password con risposte articolate e non banali (evitare nomi del proprio cane, gatto, ecc…).
La condivisione del materiale multimediale e delle informazioni personali che riguardano la presenza di altre persone richiedono necessariamente il consenso espresso e documentato di ciascun individuo presente, al fine di non incorrere in azioni legali da parte di questi per il mancato consenso. 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.
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 guidate da compiere direttamente su un form gestito dal sito. Prima di trasformare un incidente o una "bravata" in una denuncia alle autorità competenti, bisognerebbe avvalersi della modalità di segnalazione che non espongano le parti in causa a conseguenze penali e giudiziarie che si protraggono per anni.

Comportamenti nelle relazioni tra persone di pari livello – (Rapporto 1 a 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 nello spazio virtuale, evitando di condividere riferimenti personali e di contatto, come numeri di telefono o indirizzi, dati che nei contesti della vita reale sarebbero considerati privati e strettamente personali. 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.
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.
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 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 creandone uno nuovo.
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.
E' buona prassi per l'utente non aprire mai dei file sospetti, verificandone l'attendibilità con un antivirus aggiornato; la maggior parte dei programmi P2P contiene spyware e malware, software malevoli in grado di compromettere l'integrità dell'ambiente operativo. Per motivi di sicurezza della rete l'utilizzo questi sistemi a scuola è vietato.
La stessa accortezza dovrà essere prestata alle regole della posta elettronica al fine di preservare la privacy di tutti, è importante pertanto aver cura di cancellare il mittente o occultare i diversi destinatari quando si invia un messaggio condiviso con più utenti , evitare di inoltrare spam o catene di sant'Antonio, o perpetrare qualunque tipo di

abuso usando i messaggi elettronici.
Quando si scambiano contenuti multimediali o si pubblicano video con colonne sonore o musiche 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)

La condivisione dei contenuti sulle applicazioni dei Social Network consentono l'accesso a diversi gradi di condivisibilità, è compito dell'utente gestire il corretto livello di privacy per ogni singolo elemento condiviso e diffuso in Rete; 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.
L'utente accorto conosce il pericolo insito nella rete e la diffusione ramificata delle informazioni diffuse, è buona prassi quindi evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato.
Il materiale messo in condivisione deve sempre rispettare le regole predisposte dalla community, è severamente vietata la condivisione di materiale considerato inappropriato all'ambiente dagli amministratori del sito e sanzionato, talvolta con l'espulsione, se contravvenute le regole di un corretto utilizzo.
Se si usa un nuovo servizio messo a disposizione dal Social Network, bisogna informarsi su quali siano gli strumenti per segnalare materiale e comportamenti inadatti, e quali le modalità corrette per denunciare un sopruso. Se un contenuto viene moderato e non è più visibile online, probabilmente esso non è stato reputato idoneo. E' necessario sempre accertarsi di utilizzare un linguaggio non offensivo nei confronti degli altri fruitori della community e se il contenuto sia adeguato a un determinato spazio condiviso. 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)

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 selezionare le relazioni di scambio e 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.
E' importante prestare particolare attenzione alle amicizie nate nel contesto virtuale: bisogna evitare di condividere contatti, dati personali e contenuti privati, soprattutto se riguardano terze persone. La rete sociale non è facile da controllare quindi è necessario ricordare 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. 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. La reputazione digitale è persistente e si diffonde velocemente pertanto non si dovrebbero 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 ITC

Rete di Istituto, servizi e postazioni informatiche
Sicurezza nell'uso delle ITC 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;
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 il meccanismo di profilo mobile di Windows, che archivia centralmente sul server di dominio i dati, e li rende disponibili in tutti gli spazi riservati alla didattica (laboratori, sale insegnanti, postazioni per studenti e docenti). Su dispositivi di proprietà della scuola, 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 di backup automatico su NAS.

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 il riconoscimento degli utenti dietro richiesta di credenziali (nome utente e password).
L'ottenimento delle credenziali è riservato a studenti e personale dell'Istituto. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

Linee guida di utilizzo delle ITC per Studenti e Docenti

Studenti
Al fine del corretto utilizzo degli spazi digitali messi a disposizione della scuola, gli studenti si impegnano a rispettare scrupolosamente alcuni precetti fondamentali, quali:
non è permesso utilizzare giochi né in locale, né in rete;
si devono sempre salvare 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;

è necessario mantenere riservata l'identità personale e non rendere noti dati, come: il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della vostra scuola;
non si può inviare o condividere fotografie proprie e di compagni; bisogna consultare sempre il parere di un tecnico o un insegnante prima di scaricare documenti da Internet o prima di effettuare registrazioni a siti o di sottoscrivere iscrizioni;si deve riferire sempre all'insegnante qualsiasi tentato accesso da parte di terzi al proprio account o la condivisione di materiale non idoneo, sia recapitato che incontrato in navigazione di siti; è necessario informare tempestivamente il docente o un familiare adulto di eventuali richieste di incontri con persone conosciute in ambiente virtuale; è sempre opportuno la verifica dell'adulto in questi casi, ritenendo pericolosi certi atteggiamente; non è consigliabile inviare mail personali, bisogna rivolgersi sempre all'insegnante prima di inviare messaggi di classe;
non si può scaricare o copiare materiale da Internet senza il permesso di un docente o un responsabile di laboratorio.

Docenti
Anche il corpo docenti deve attenersi alle regole che disciplinano l'utilizzo dell'ambiente multimediale nei locali della scuola.
E' importante che essi:
Evitino di lasciare le e-mail o file personali sui computer o sul server della scuola, in quanto lo spazio è limitato;
salvino sempre i 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;
illustrino ai propri studenti PUA della scuola e gli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
diano chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informino sulle strategie di tutela e monitoraggio della navigazione da parte dell'Istituto; verifichino lo stato dei computer alla fine della sessione di lavoro, in particolare controllando che siano tutti spenti all'uscita dall'ultima ora di lezione;
ricordino 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. 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 dell'Animatore Digitale. La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato richiesto 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 ITC della scuola
Informazione del personale scolastico
Le regole di base relative all'accesso ad Internet, sono considerate parte integrante del regolamento d'Istituto, esse sono pubblicate sul sito e sono affisse 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 ITC sottoscrivendola all'inizio dell'anno scolastico, alla sottoscrizione del rapporto di lavoro ed ogni qualvolta vi sarà apportata una variazione, sempre tenendo conto che l'uso della rete sarà sottoposto a monitoraggio.

Informazione degli alunni
Sarà cura dell'Animatore digitale e poi del docente responsabile del laboratorio e dei vari fruitori, 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 in merito alle 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:

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 compie il medesimo fatto mediante comunicazione telegrafica o telefonica o con scritti, o disegni, diretti alla persona offesa.

DIFFAMAZIONE

E' da considerarsi atto diffamatorio, qualsiasi comportamento assunto per offendere: " [...] 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 arrecata con un "mezzo di pubblicità" come l'inserimento, ad esempio, in un sito Web o social network di un informazione o un giudizio su un soggetto.
La pubblicazione on-line dà origine ad un elevatissimo numero di "contatti" di utenti della Rete, generando un' incontrollabile e inarrestabile diffusione della notizia.

MINACCE E MOLESTIE

Il reato di minaccia consiste nell'indirizzare ad una persona scritte 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

Per far fronte alla violazione delle regole stabilite dalla politica scolastica, la scuola si impegna formalmente a valutare e a procedere attraverso l'operato del responsabile di laboratorio e del Dirigente Scolastico per impedire l'accesso dell'utente contravventore a Internet per un certo periodo di tempo, rapportato alla gravità dell'infrazione commessa.

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 al fine di renderlo nuovamente operativo e 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.