Ministero dell'Istruzione, dell'Università e della Ricerca
Istituto Comprensivo Statale Travagliato

Via IV Novembre 2 - TRAVAGLIATO
Tel. 030 660242 – Fax 030 6864241
bsic89200c@istruzione.it pec: bsic89200c@pec.istruzione.it
Codice Fiscale 98169490178

POLICY AND E-SAFETY

Sommario

POLICY AND E-SAFETY

Introduzione

Fa riferimento a un insieme di regolamenti, linee di azione e attività poste in essere per fare fronte ad una serie di necessità individuate. Una policy non è mai il risultato di un'azione unica, quanto piuttosto l'esito delle interazioni di un insieme di azioni e decisioni.

Comprende:

1. Le misure di prevenzione e misure di gestione di situazioni problematiche relative all'uso delle tecnologie digitali (azioni finalizzate alla prevenzione nella scuola di fenomeni legati ai rischi delle tecnologie digitali che includano iniziative volte a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, dell'utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC, ecc.).
2. Le misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici (azioni utili a sviluppare le competenze digitali, che costituiscono anche misure di prevenzione).
3. Misure per la segnalazione dei casi, ossia disposizioni semplici su come segnalare i casi nella scuola, comprese informazioni su chi sono le figure di riferimento, sugli strumenti a disposizione, sull'iter successivo alla segnalazione e su quali misure di tutela può contare chi segnala.
4. Misure per la gestione dei casi ovvero le misure che la scuola attiva a supporto delle vittime, degli aggressori, delle famiglie e di tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto; misure che disciplinano anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali.

1. Fra gli utenti dei servizi telematici Internet, si sono sviluppati nel corso del tempo una serie di principi di buon comportamento (galateo)che vengono identificati con il nome di Netiquette 2.0.
2. 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.
3. Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, Netlog, ecc. …, 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.
4. Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa mantenere 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.).
5. Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non bisogna pubblicare su YouTube video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.
6. 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.
7. 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)

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.

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 creandosene uno nuovo. (Vedi capito5 Help line e privacy)

I sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica quindi è necessario preservare la privacy di tutti, cancellando il mittente o i vari destinatari quando si invia un

messaggio a più destinatari che non si conoscono tra loro, evitare di inoltrare spam o catene di sant'Antonio, o perpetrare qualunque tipo di abuso usando i messaggi elettronici.

Quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica di sottofondo bisogna essere sicuri di averne il diritto d'uso e di non utilizzare alcun file coperto da copyright.

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

Dal momento che ciò che viene pubblicato su un Social Network è persistente e spesso non è facile da cancellare, bisogna evitare di postare materiale che in futuro non si vorrebbe veder pubblicato.

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

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.

CAPITOLO2 – Formazione e curricolo

Curricolo sulle competenze digitali per studenti

Il concetto di competenza fa riferimento alla capacità del soggetto di mobilitare le proprie risorse interne, in termini ad esempio di emozioni, ma anche di abilità e conoscenze, e integrarle con quelle esterne per agire all'interno di un contesto dato e risolvere situazioni problematiche.

Guardare all'apprendimento da questa prospettiva significa interpretarlo come un processo dinamico di costruzione della conoscenza, non più intesa come insieme di nozioni e contenuti statici.

Non stupisce che tra le competenze di base europee sia stata individuata quella di "imparare a imparare", una competenza metodologica, trasversale, che si fonda sulla capacità di riflettere sui punti di forza e di debolezza del proprio apprendimento.

Cosa significa essere competenti quando parliamo di ICT?

Dimensione tecnologica: questo ambito fa riferimento a una serie di skill tecnologiche di base, come ad esempio la conoscenza di dispositivi e interfacce, ma comprende anche livelli più avanzati legati alla capacità di valutare le potenzialità dei contesti tecnologici in trasformazione, imparando a selezionare le soluzioni più opportune per affrontare ciascun compito;

Dimensione cognitiva: comprende abilità legate al trattamento dell'informazione, dalla capacità di accedere, selezionare e interpretare dati a quella di valutarne criticamente la pertinenza e l'affidabilità, ma anche il saper trattare testi e dati per produrne sintesi, analisi e rappresentazioni con tabelle e grafici;

Dimensione etica: questa dimensione riguarda il saper interagire con gli altri in modo corretto e responsabile, la circolazione del sapere online e il rispetto dei diritti di proprietà intellettuale, il tema dell'accessibilità e dell'inclusione. Comprende alcune delle tematiche più attuali rispetto al tema delle nuove tecnologie, dalla tutela della privacy al contrasto del fenomeno del cyberbullismo, e quelle che riguardano la dimensione relazionale ed affettiva dell'utilizzo di internet: il fatto di non vedersi e di non sentirsi direttamente, o di non entrare in contatto visivo, abbassa timidezze e inibizioni, per cui spesso nella comunicazione in rete si raggiungono elevati livelli di confidenza e intimità e a volte, di seduttività, proprio perché l'altro/a può essere uno sconosciuto e come tale, liberamente immaginato e idealizzato.

- Lettore: capacità di leggere i messaggi mediali, smontandoli per individuare regole, codici e generi;
- Scrittore: capacità di produrre messaggi mediali, con tutto quel che questo comporta in relazione alla responsabilità dell'essere autore e del rappresentare.
- Critico: capacità di comprendere valori e punti di vista veicolati dai media, sviluppando senso critico rispetto alla dimensione etica e socio-culturale;
- Fruitore: capacità di operare scelte consapevoli di consumo mediale, riflettendo sui propri bisogni e generando consapevolezza delle implicazioni e delle alternative;
- Cittadino: capacità di abitare i media come spazi di relazione e di costruzione di cultura e partecipazione.

Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

La didattica digitale sembra potersi sposare con la modalità della scuola-laboratorio, in cui il momento teorico non precede quello pratico: è possibile quindi privilegiare approcci di tipo **learning by doing.** Nel modello della **flipped-classroom** i momenti vengono invertiti: la lezione avviene a posteriori, dopo che lo studente ha provveduto in via preliminare all'acquisizione delle informazioni di base. Questa inversione è suggerita dall'attuale contesto informativo e dalla diffusione di fonti di conoscenza: attraverso risorse digitali libere e di reti sociali educative, per la fase preliminare sarà possibile avvalersi di materiali liberamente accessibili ed utilizzabili, quali video didattici, podcast, strumenti interattivi. Dislocare la spiegazione iniziale

fuori dalle mura scolastiche permette di organizzare in classe attività di approfondimento, riflessione, applicazione, ad esempio attraverso discussioni su eventuali dubbi, attività di gruppo e problem solving. Ed è quindi qui che si colloca effettivamente il potenziale innovativo di questo metodo, che va ad incentivare una didattica di tipo costruttivista. Secondo i fautori di questo metodo, le ricadute sull'apprendimento sono consistenti, sia perché lo studente ha una maggiore flessibilità e personalizzazione nei tempi e modi di apprendimento, sia perché il ribaltamento **"learn at home, study at school"** permette di liberare tempo in classe per attività cognitive più complesse e riflessive**.**

EAS – Episodi di apprendimento situato

- **fase preparatoria**: è a carico dell'insegnante, che introduce le informazioni preliminari, organizza il setting e fornisce uno stimolo e una consegna da svolgere, specificando gli strumenti tecnologici da utilizzare;
- **fase operatoria**: gli studenti portano a termine la consegna, elaborando un prodotto finito;
- **fase ristrutturativa**: è dedicato alla condivisione e al debriefing, in cui gli studenti riflettono sul proprio operato sotto la guida dell'insegnante, acquisendo consapevolezza di quanto emerso e fissando gli aspetti più importanti.

Da un punto di vista didattico, si lavora sull'integrazione di strategie di problem solving, learning by doing e reflective learning. Ciascuna fase è oggetto di valutazione da parte dell'insegnante (embedded assessment), che non valuta solo i prodotti finiti ma anche le competenze trasversali messe in campo dagli studenti come il lavoro di gruppo e la competenza digitale.

Formazione dei docenti

All'interno del PTOF viene individuata una persona (formatore informatico) con l'incarico di aggiornare e stimolare alla formazione i docenti; fornirà elenchi aggiornati di corsi online o in presenza, terrà corsi di aggiornamento e farà da facilitatore all'utilizzo delle TIC nella didattica e una equipe di supporto formata da tre insegnanti e due addetti di segreteria.

Sensibilizzazione delle famiglie

Attraverso il Registro elettronico in adozione nella scuola le famiglie verranno aggiornate sugli eventi e sulle attività in atto e avranno la possibilità di interagire esprimendo pareri o portando esperienze anche usando lo spazio genitori creato in DRIVE

CAPITOLO 3 – Sicurezza e Uso delle TIC

Rete di Istituto, servizi e postazioni informatiche

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

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

- il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso e l'uso della rete interna ed esterna (Internet) secondo i normali canali di protezione presenti nei sistemi operativi e utilizzando, se necessario, software/hardware aggiuntivi come Firewall;

- si attrezza per evitare comportamenti che non rientrano nelle norme che il collegio dei docenti delinea in proposito come:

- Scaricare file video-musicali protetti da copyright;
- Visitare siti non necessari ad una normale attività didattica;
- Alterare i parametri di protezione dei computer in uso;
- Utilizzare la rete per interessi privati e personali che esulano dalla didattica;
- Non rispettare le leggi sui diritti d'autore;
- Navigare su siti non accettati dalla protezione interna alla scuola.

Disposizioni, comportamenti, procedure:

Il sistema informatico è periodicamente controllato dai responsabili;

La scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina;

La scuola archivia i tracciati del traffico Internet (log del software proxy principale);

E' 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 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;

E' vietato utilizzare e-mail personali ad uso privato durante le ore di lezione;

E' vietato l'utilizzo delle postazioni durante le ore di lezione per motivi non strettamente legati alla pratica didattica;

E' 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;

E' 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 con SO Windows sono protette con sistemi antivirus regolarmente aggiornati.

La memorizzazione dei documenti trattati dalle postazioni degli uffici è garantita mediante archiviazione sul server di dominio su cui è attivo un servizio regolare di backup. Le altre postazioni (studenti, docenti, esterni) sono da considerarsi come strumenti di lavoro su cui non va salvato alcun dato. Si consiglia di fare copia su un supporto personale (pen drive, cd o altro) dei propri dati.

Sicurezza della rete senza fili (Wireless – Wi-Fi)

L'Istituto (scuola secondaria) 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 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 TIC per Studenti e Docenti

Studenti

Non utilizzate giochi né in locale, né in rete;

Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione 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 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;

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 Policy 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 Policy 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: www.ictravagliato.gov

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

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

CAPITOLO 4 – Informazione

Informazione sulla Politica d'Uso Accettabile delle TIC della scuola-uso strumentazione personale

Informazione del personale scolastico

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

CAPITOLO 5 – Disposizioni di legge e sanzioni - Reati e violazioni della legge

Rilevazione

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 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, 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.

Azioni-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.

Reati per cui si procede d'ufficio

- ISTIGAZIONE E DELINQUERE (414 c.p.);
- ATTI OSCENI (527 c.p.);
- ISTIGAZIONE AL SUICIDIO (580 c.p.);
- RISSA (588.c.p.);
- VIOLENZA SESSUALE (609bis C.P.);
- PORNOGRAFIA MINORILE (600ter- attenzione al 609quater co.4: non è punibile il minorenne che, al di fuori dei casi del 609bis, compie atti sessuali…);
- VIOLENZA PRIVATA (610 C.P.);
- VIOLENZA O MINACCIA PER COSTRINGERE A COMMETTERE UN REATO (611 C.P.);
- ATTI PERSECUTORI (612bis);
- FURTO CON STRAPPO (624bis);
- RAPINA (628 c.p.);
- ESTORSIONE (629 c.p.)

Reati procedibili a querela della Polizia Postale

- PERCOSSE (581 c.p.);
- LESIONI PERSONALI (582c.p.- fino a 20gg. di prognosi);
- INGIURIA (594 c.p.);

- DIFFAMAZIONE (595 c.p.);
- MINACCIA (612 c.p. – se è grave, si procede d'ufficio);
- INTERFERENZE ILLECITE NELLA VITA PRIVATA (615 bis c.p.);
- FURTO (624 c.p.);
- DANNEGGIAMENTO (635 c.p.- eccetto comma 2);

Helpline e privacy

Gestione dei casi

Definizione delle azioni da intraprendere a seconda della specifica del caso.

Qualora si riscontri una delle violazioni presentate nel capitolo 5 o si sia a conoscenza di atteggiamenti o uso delle tecnologie non conformi con la policy della scuola segnalarle tempestivamente al Dirigente scolastico, al vicedirigente o all'Animatore digitale in modo che si possa procedere.

Se subisci ricatti o diffusione di foto e messaggi privati rivolgiti agli operatori del **Servizio di helpline** facendo il numero telefonico **1.96.96 gestito da Telefono Azzurro** nell'ambito del progetto Generazioni Connesse.

Gli operatori sono disponibili ad offrirti uno spazio confidenziale di ascolto e di aiuto anche attraverso la **chat presente sul sito** www.azzurro.it/chat.

Il servizio telefonico è attivo 24 ore su 24; la chat è invece operativa tutti i giorni dalle 8 alle 22, il sabato e domenica fino alle 20.

Siti Web dai contenuti illeciti o contatti con persone sospette devono essere segnalati alla Polizia Postale e delle Comunicazioni all'indirizzo: www.commissariatodips.it

Il 114 è il numero di emergenza al quale rivolgersi tutte le volte che un bambino è in pericolo; è attivo 24 ore su 24, sette giorni su sette, è gratuito ed è raggiungibile sia dal telefono di casa che dal telefono mobile. Il sito **www.114.it** consente di accedere a materiali utili in caso di violenza di qualsiasi tipo sui minori; è possibile anche accedere alle FAQ.

Se qualcuno riceve insulti dal tuo profilo Facebook (e tu non sei l'artefice dei messaggi) vuol dire che sono riusciti a scoprire la password di accesso al suo account.

Devi chiamare 19696 e farti aiutare ad impostare correttamente la **privacy in Facebook** e formulare una nuova password che ti consenta di mantenere privati i dati personali.

Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio. Devi parlarne con i genitori affinché segnalino l'accaduto alla **Polizia Postale**.

Si segnalano anche i riferimenti di alcune Associazioni che si occupano delle problematiche relative allo sfruttamento dei minori a scopo sessuale e che hanno collaborato, in alcune occasioni, con la Polizia Postale e delle Comunicazioni:

Lo Sportello "Help Web Reputation Giovani" istituito da Co.Re.Com Lombardia nell'ambito della delega relativa alla tutela dei minori e delle problematiche connesse al corretto utilizzo della Rete da parte dei giovani. **www.corecomlombardia.it**

ECPAT - www.ecpat.it - info@ecpat.it
METER - www.associazionemeter.it - segnalazioni@associazionemeter.org
MOIGE - www.genitori.it - redazionemoige@genitori.it
Save the Children - stop-it@savethechildren.org
Telefono Azzurro - www.azzurro.it
UNICEF – www.unicef.it - info@unicef.it

Procedure operative per la gestione delle infrazioni alla Policy.

Furto d'identità:

Impedimento all'utilizzo dell'account

Lettura di informazioni personali

Uso dei dati per accesso a siti in cui si è registrati

Invio di mail a mio nome

Truffe a mio nome (eBay – subito.it - kijiji).

Procedure operative per la protezione dei dati personali

Non far ricordare la password al tuo pc

Digitala ogni volta personalmente per non avere brutte sorprese

Usa password difficili da indovinare utilizzando caratteri alfanumerici e/o caratteri speciali, lunghe almeno 8 caratteri e sostituite regolarmente

Se hai il dubbio che qualcuno possa aver scoperto la tua password cambiala subito.

Non condividere la tua password con nessuno

In quali casi il Corecom (Comitato Regionale Comunicazioni) può intervenire

- Articoli o notizie pubblicati su blog o siti;
- Foto o immagini offensive o diffamanti all'interno di social network;
- Commenti offensivi all'interno di social network;
- Diffusione non autorizzata di scritti personali o di corrispondenza;
- Post all'interno di forum;
- Video offensivi o diffamatori;
- Furto d'identità.

Reati contro la persona e contro i minori commessi in ambito informatico:

Il quadro normativo italiano

L.269/98 – L.38/06 – L-172/12 - Norme sulla pedopornografia on line

Art.595 c.p. – Diffamazione

Art.612 bis c.p. –Atti persecutori

Art.494 c.p. – Sostituzione di persona

Art.167 d.leg196/03 – Uso indebito dati personali

Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.

I genitori devono essere informati dei comportamenti scorretti messi in atto dai figli in orario scolastico ed essere resi partecipi delle misure punitive e/o riabilitative che si intenderanno adottare nei confronti dei minori.

Con la firma **del PATTO DI CORRESPONSABILITA'** "I genitori si assumono l'impegno di rispondere direttamente dell'operato dei propri figli …. *omissis*" (Circolare del 15 Marzo 2007, Ministero della Pubblica Istruzione, DPR 235 del 2007)

Lo studente, deve essere punito con comportamenti attivi di natura risarcitoria e riparatoria, volti al perseguimento di una finalità educativa (Circolare del 15 Marzo 2007, Ministero della Pubblica Istruzione, DPR 235 del 2007)

Reati subiti all'interno di chat-room

E' opportuno fornire il testo della conversazione con riferimenti illegali avuta in chat (se conservato), indicazioni precise di data e ora, del nickname dell'utente, delle caratteristiche della chat usata, dei log delle conversazioni, ecc.

Reati subiti collegati all'utilizzo di SOCIAL NETWORK

E' opportuno fornire indicazione esatta del social network adoperato, profilo utente, messaggio/fotografia con contenuto illecito, dati di inserimento, log delle conversazioni, ecc.

- Procedure operative per la gestione dei casi.

Se il minore chiede direttamente aiuto ad un insegnante la **SCUOLA**, può segnalare anche direttamente alla Procura della Repubblica presso il Tribunale per i Minorenni la situazione.

In caso di un minore che con i suoi comportamenti gravi manifesti un disadattamento sociale che faccia temere la caduta nella devianza vera e propria la **SCUOLA**, può segnalare anche direttamente alla Procura della Repubblica presso il Tribunale per i Minorenni la situazione.

La scuola istituisce **un registro** delle segnalazione dove si riportano le denunce pervenute e gli eventuali sviluppi e le sanzioni applicate. Il Protocollo di Intesa del 2004 Art. 13 sancisce che il Dirigente scolastico e gli insegnanti devono evitare mortificazioni, garantire riservatezza sulle confidenze ricevute e dare immediata notizia all'Autorità Giudiziarie.

Competenze del tribunale dei minori: decide questioni che riguardano la tutela dei minori e interviene quando i genitori non adempiono ai loro doveri (mantenimento, educazione e istruzione…);

Il T.M., può porre limiti all'esercizio della potestà genitoriale;

Attiva l'intervento dei servizi sociali;

Può allontanare il minore dalla casa familiare e affidarlo temporaneamente ad altra famiglia, istituto…

Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

Art. 14 Collaborazione tra Dirigenti Scolastici e Forze dell'Ordine