I.I.S. “Guglielmo Gasparrini” - MELFI

# Regolamento utilizzo rete LAN e WiFi

# E-Safety Policy

Approvato nella seduta del Consiglio d’Istituto del 10 aprile 2020

## INDICE

## Art. 1 – Premessa

Il presente regolamento, parte integrante del Regolamento d'Istituto dell'I.I.S. "G. Gasparrini", si applica alle modalità di utilizzo della rete LAN (Local Area Network), al sistema di connessione Wi-Fi e all'uso dei sistemi telematici (Internet) nelle attività inerenti la produzione di materiale con finalità didattiche, lo scambio/recupero di documenti e informazioni dalla rete internet e lo sviluppo di soluzioni che permettano l'interazione di tutti i soggetti inseriti nel contesto operativo scolastico.

Internet offre sia agli studenti che agli insegnanti una vasta scelta di risorse e di opportunità di pubblicazione e scambio.

Per gli studenti e per gli insegnanti l'accesso alla rete web a scuola deve essere effettuato nel rispetto di quanto riportato nelle disposizioni del Ministero dell'Istruzione Università e Ricerca che vietano l'uso in classe di telefoni cellulari e dispositivi elettronici. (Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, … http://archivio.pubblica.istruzione.it/normativa/2007/allegati/prot30_07.pdf)

Nella possibilità che gli alunni trovino materiale inadeguato e/o illegale su internet, la scuola ha limitato l'accesso alla rete mediante un sistema di protezione e di sicurezza informatica (Firewall) che permette di filtrare, monitorare e tracciare le attività svolte in rete nel rispetto delle vigenti normative sulla privacy. Con questo sistema pertanto si ha la possibilità di filtrare ciò che arriva attraverso Internet sulla base di criteri relativi alla sicurezza informatica e limitare gli utilizzi della rete vietando la connessione a determinate categorie di siti ritenuti non affidabili o pericolosi. Questa soluzione non è però in grado di eliminare tutti i rischi in quanto è possibile commettere errori, compiere azioni non legali su siti comunque raggiungibili o intraprendere attività ritenute non lecite attraverso una connessione ad Internet priva di protezione ovvero utilizzando il proprio cellulare/device.

In ultimo si pone in particolare evidenza la necessità di promuovere negli alunni la cultura del rispetto di regole comuni anche nell'uso dei servizi telematici (Internet). A tal proposito sono state sviluppate, nel corso degli anni, numerose regole di buon comportamento identificate con il nome di Netiquette (neologismo sincratico che unisce il vocabolo inglese network-rete e quello di lingua francese étiquette-buona educazione). Con l'avvento del web 2.0 e della diffusione dei Social Network, basati su principi di collaborazione e condivisione diretta degli utenti, internet e i suoi servizi si sono evoluti dando vita ad un galateo del web 2.0 al quale tutti i netizen (cittadini della rete) devono fare riferimento e che va collettivamente rispettato. Stiamo parlando delle Netiquette 2.0 (http://it.wikipedia.org/wiki/Netiquette). 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.

Scopo di questo regolamento è quello di guidare gli studenti nelle attività on-line, stabilire le regole nell'uso di internet ed educare un nuovo modello nell'utilizzo responsabile degli strumenti di intercomunicazione digitale.

Nel regolamento sono riportate le indicazioni utili a tutelare la sicurezza di tutti gli utenti della rete, lo stesso è pubblicato sul sito del nostro istituto, viene sottoscritto dagli studenti e dai docenti che richiedono le credenziali per l'accesso alla rete wireless.

Tutti gli utenti della rete dell'Istituto d'Istruzione Superiore "G. Gasparrini" sono tenuti a rispettare scrupolosamente questo regolamento, 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.

## Art. 2 - Principi Generali

Quali principi generali cui attenersi in termini di etica e di buon uso dei servizi di rete, l'Istituto d'Istruzione Superiore "G. Gasparrini" ha deciso di prendere come riferimento i principi proposti dal Ministero dell'Istruzione Università e Ricerca nel documento che riassume "La posizione italiana sui principi fondamentali di Internet

### Principi fondamentali di Internet

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

#### a. Principi generali

Internet bene comune. I protocolli di Internet sono bene comune inalienabile, a garanzia della sopravvivenza stessa della rete. Essi rimangono a disposizione dei diversi attori che operano in Internet, siano essi società civile, imprese o istituzioni pubbliche e rappresentano una risorsa comune che ampliando l'offerta culturale e le possibilità di condivisione di conoscenza, arricchisce la collettività e favorisce il progresso sociale ed economico.

Internet è strumento cruciale per lo sviluppo e l'esercizio dei diritti umani.

Internet, in quanto risorsa globale di interesse pubblico, è uno strumento economico e di facile uso.

È ubiquo e presente su tutto il territorio nazionale, tecnicamente in grado di supportarne la fruizione da parte di tutti gli utenti. Se questi requisiti sono soddisfatti, Internet è uno strumento essenziale per lo sviluppo e il conseguimento dei diritti fondamentali.

Neutralità della rete e architettura aperta.

La neutralità della rete costituisce una garanzia che il futuro di internet mantenga quei requisiti di apertura, di competitività e di innovazione che hanno consentito il suo successo.

Benefici della tecnologia e della rete.

Lo Stato riconosce che i cittadini devono poter beneficiare dei progressi della tecnologia digitale e delle sue applicazioni. Tali tecnologie possono contribuire in modo sostanziale a migliorare l'efficienza e l'efficacia dei servizi pubblici essenziali offerti dallo Stato, quali istruzione, giustizia e sanità, nonché ad ampliare le possibilità e le modalità di partecipazione democratica.

Modello decisionale trasparente con il coinvolgimento di tutti i portatori di interesse ("stakeholder"). La governance di Internet è trasparente (i processi decisionali avvengono

pubblicamente) e flessibile (vale a dire in grado di adattarsi alle esigenze, in continua evoluzione, del contesto globale), e si avvale degli strumenti della cooperazione internazionale.

### b. Cittadinanza in rete

Accessibilità come strumento di inclusione. La fruizione di strumenti e piattaforme della rete avviene senza limitazioni o barriere tecniche all'entrata per tutti i cittadini, in particolare alle persone con disabilità. I contenuti e i servizi in rete della pubblica amministrazione sono accessibili a tutti, senza alcuna discriminazione, in particolare alle persone che per disabilità o condizioni particolari (es: divario digitale) non possono interagire con le amministrazioni se non tramite l'uso di Internet.

Diritti umani e libertà fondamentali in rete e per mezzo della rete. Nel rispetto dello stato di diritto, le istituzioni incoraggiano l'uso globale della rete Internet e delle sue applicazioni in quanto strumenti di partecipazione democratica e promozione dei diritti umani e delle libertà fondamentali tra cui quelle di opinione, espressione, informazione, riunione e associazione.

Auto-organizzazione e autonomia degli individui in rete.

Internet costituisce un luogo privilegiato di sperimentazione, scambio di conoscenze e pratiche sociali. Tali pratiche sono incoraggiate quali spazi di innovazione sociale, partecipazione dal basso ed esempio concreto di esercizio della cittadinanza digitale.

### c. Consumatori e utenti della rete

Competenze digitali. Le istituzioni pubbliche, e in particolare il sistema educativo, favoriscono l'acquisizione e l'aggiornamento continuo delle competenze digitali nei diversi settori della società, con particolare riguardo alla eterogeneità di esigenze ed abilità dei potenziali utilizzatori, senza discriminazione di soggetti appartenenti a categorie deboli o svantaggiate. Le competenze informatiche sono intese come educazione all'impiego delle tecnologie e all'uso critico e consapevole dell'infrastruttura e dei suoi strumenti, applicando modelli di riferimento internazionali per l'identificazione delle competenze e professionalità. Identità digitale. L'identità personale ha una sempre maggiore componente digitale, e la sua tutela comprende, tra gli altri fattori, anche la promozione della consapevolezza dell'utente delle tracce informative memorizzate in rete ("ombre informative"). La creazione di un'identità digitale è un elemento essenziale per la creazione di rapporti commerciali e sociali affidabili, per il tracciamento delle attività illegali e per la riservatezza delle informazioni personali e delle comunicazioni interpersonali.

Riservatezza. L'interazione in rete, e in particolare nelle reti sociali, genera flussi di dati e di relazioni (grafi sociali) di rilievo a disposizione dei gestori delle piattaforme e dei loro partner. La raccolta e l'uso di informazioni sulla persona a scopo commerciale è regolata nel rispetto del diritto della persona alla riservatezza e attraverso lo sviluppo di approcci condivisi tra utenti, fornitori di servizi, istituzioni ed enti regolatori.

### Accesso, archiviazione e cancellazione dei dati personali.

I dati personali appartengono all'utente, il quale è portatore del cosiddetto "diritto all'oblio", vale a dire la possibilità di richiedere la cancellazione di informazioni e dati personali presenti negli archivi, anche online.

## d. Produzione e circolazione dei contenuti

Condivisione dei contenuti e della conoscenza in rete. Internet rappresenta un'opportunità senza precedenti per la condivisione di informazione e conoscenza. I fornitori di servizi online, piattaforme e contenuti non proibiscono agli utenti di usare Internet per l'apprendimento condiviso e la creazione di contenuti. La tutela dei diritti dei creatori di contenuti è coerente con il diritto degli utenti di essere parte attiva ai flussi di conoscenza culturale e scientifica.

Proprietà intellettuale in ambiente digitale. Diritto d'autore, marchi, brevetti e segreto commerciale sono tutelati secondo le disposizioni dei trattati internazionali, e attraverso lo strumento della cooperazione internazionale. Si tutelano il diritto alla copia personale, alla citazione e al riuso della conoscenza in rete.

## e. Sicurezza in rete

Sicurezza in rete. Adeguate misure sono adottate per assicurare l'integrità della rete e il suo uso non malevolo o per fini terroristici e criminali, salvaguardando al tempo stesso il suo uso nell'esercizio della libertà di espressione.

Internet, comunicazione di crisi e operazioni di soccorso. Lo Stato tutela e promuove l'uso creativo della rete e delle sue applicazioni da parte delle istituzioni pubbliche e delle forze di pubblica sicurezza nella gestione e prevenzione dei disastri e delle catastrofi naturali, al fine di preparare la popolazione (preparedness messaging), aumentare l'efficienza delle operazioni di soccorso e facilitare l'accesso dei cittadini ad informazioni affidabili nell'emergenza.

Protezione dei soggetti deboli. Internet, oltre a costituire un'opportunità, presenta potenziali rischi per alcune fasce deboli della società, quali ad esempio i minori, i soggetti con divario digitale, persone con disabilità, stranieri, e cittadini con limitate competenze informatiche. A tale riguardo se ne promuove l'uso critico e consapevole da parte degli utenti, e si ostacolano le pratiche di abuso dello strumento, anche attraverso pratiche di auto-regolamentazione, quali ad esempio il già esistente Codice di Autoregolazione degli Operatori di Accesso.

## Art. 3 – Ruoli e responsabilità

### Dirigente scolastico

Il Dirigente scolastico promuove l'uso delle tecnologie e di internet e deve:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

### Animatore digitale

All'Animatore digitale spetta il compito di:

- stimolare la formazione interna in riferimento a quanto contenuto nel PNSD e nel PTOF;
- fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la "scuola digitale".

### Responsabile del sito web dell'Istituto

Al responsabile del sito web dell'Istituto spetta il compito di:

- curare la manutenzione e lo sviluppo del sito web, garantendo la visibilità on-line esclusivamente per i fini istituzionali della scuola;
- promuovere nella comunità scolastica la formazione di un gruppo di lavoro che segua e aggiorni costantemente le notizie ed i documenti pubblicati;
- garantire la manutenzione e la riservatezza degli account assegnati al personale autorizzato alla pubblicazione sul sito;
- garantire la conformità, di quanto pubblicato on-line, relativamente alle e-policy dell'Istituto.

### Responsabile della rete interna (LAN e WiFi) dell'Istituto

Al responsabile della rete interna (LAN e Wifi) dell'Istituto spetta il compito di:

- manutenere la rete interna (LAN e WiFi) dal punto di vista logico (non fisico - impiantistico) razionalizzando le politiche di accesso, segmentazione e bilanciamento del traffico;
- assicurare che tutti gli utenti possano accedere alla rete della scuola solo tramite password periodicamente cambiate;
- curare la sicurezza della rete mediante misure di prevenzione da attacchi virali e tentativi di intrusione provenienti dall'esterno;
- monitorare le attività svolte dagli utenti autorizzati all'interno della rete;
- sensibilizzare la comunità scolastica al rispetto delle norme contenute nel presente regolamento.

### Direttore dei servizi generali e amministrativi

Il direttore dei servizi generali e amministrativi deve:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola per la notifica dei documenti e delle informazioni istituzionali

### Docenti

Il personale docente deve:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica, ove consentito;
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;

- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

### Alunni

Gli alunni devono:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

### Genitori

Il ruolo dei genitori degli alunni include i seguenti compiti:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet

## Art. 4 - Condivisione e comunicazione del Regolamento e della Policy all'intera comunità scolastica.

### Condivisione e comunicazione della politica di e-safety agli alunni

Tutti gli alunni devono essere informati che la rete, l'uso di Internet e di ogni dispositivo digitale di proprietà dell'Istituto e/o connesso alle reti LAN e WiFi dell'istituto è soggetto a controllo attraverso un sistema di protezione e di sicurezza informatica (Firewall) che permette di filtrare, monitorare e tracciare le attività svolte in rete nel rispetto delle vigenti normative sulla privacy. L'istituto si fa carico di istruire gli alunni riguardo l'uso responsabile e sicuro di internet attraverso diversi momenti formativi e l'attribuzione di credenziali di accesso univoche (Username e Password) di proprietà esclusiva del singolo alunno. L'elenco delle regole per la sicurezza è pubblicato on-line nel sito dell'Istituto ed è consultabile in qualsiasi momento andando nella voce "Criteri e Regolamenti". Sarà posta particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

### Condivisione e comunicazione della politica di e-safety a tutto il personale scolastico

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà portata all'attenzione degli organi collegiali e comunicata a tutto il personale. Il personale docente sarà reso consapevole del fatto che il traffico in internet è monitorato e si potrà risalire al singolo utente registrato. Azioni di informazione/formazione saranno messe in atto dall'Istituto per l'uso sicuro e responsabile di internet e delle attività connesse all'utilizzo delle TIC.

### Condivisione e comunicazione della politica di e-safety ai genitori

L'Istituto si impegna a stimolare un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali. L'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet, indirizzi web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni.

## Art. 5 – Relazioni tra persone di pari livello

Il Web 2.0 e, nel particolare, l'uso di social network hanno permesso l'attivazione di processi di comunicazione e collaborazione tra persone senza vincoli, non solo di luogo e di tempo, ma anche di conoscenza. Si è sviluppato quindi un nuovo sistema di "connessione" nel quale sono state completamente trasformate, o meglio riscritte, le regole di identità, di relazione, di comunicazione, all'interno di luoghi e contesti del tutto nuovi e non sempre conosciuti. Distinti per classi di appartenenza, migranti o nativi, siamo diventati "cittadini digitali", ma le nuove forme di cittadinanza digitale non sono automaticamente garantite a tutti. Non bastano tecnica e destrezza nell'utilizzo delle nuove tecnologie per essere o diventare cittadini responsabili, attivi e partecipativi nella società della conoscenza.

Ecco allora le regole da rispettare:

- L'utilizzo di Social Network e applicazioni web (Facebook, Twitter, Myspace, Flickr, Linkedin, YouTube, Vimeo, Foursquare, …) richiede una buona conoscenza degli articoli presenti nel regolamento d'uso, nonché dei diritti e dei doveri dell'utente.
- La condivisione di informazioni personali, immagini, contenuti, … deve essere effettuata attraverso una attenta riflessione relativa alla pubblicazione in ambiente pubblico, scegliendo con estrema cura i soggetti cui si è deciso di attribuire la propria amicizia e con cui accrescere la propria rete di conoscenze, i gruppi con cui condividere riflessioni e materiali.
- I Social Network permettono lo scambio di file con diversi utenti di cui non necessariamente si conosce l'identità, vengono richiesti nomi e cognomi reali visibili da tutti e come se non bastasse a questi dati si aggiunge un volto con una foto, iscrivendosi in qualche gruppo si forniscono anche altre informazioni come preferenze riguardo hobby, orientamenti politico/religiosi, anche il proprio numero di telefono insieme a molti altri dati sensibili.
- All'interno dei Social Network si instaurano tante relazioni tra singoli utenti, non veicolate o controllate da intermediari, chiamati rapporti di pari livello. È importante fare attenzione a quali informazioni vengono fornite in questo contesto, evitando di condividere dati personali e di contatto che nella vita reale non si darebbero a persone che non sono ancora degne di fiducia.
- Se durante una chat, un forum o in una qualsiasi discussione online, l'interlocutore diviene volgare, offensivo o minaccioso, si deve evitare l'invito a continuare la discussione e abbandonare la conversazione;
- Quando si riscontra un comportamento riconducibile ad un illecito durante una conversazione privata (tentativi di approccio sessuale, richiesta di foto, stalking o cyber bullismo) 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, se non indispensabile, abbandonare non soltanto la conversazione ma anche il profilo personale usato fino a quel momento.
- Nell'uso di sistemi di file-sharing P2P (Peer-to-peer), evitare di scaricare dei file che possono essere considerati illegali e/o protetti dal diritto d'autore, non aprire mai dei file sospetti (la maggior parte dei programmi P2P contiene spyware e malware). Per motivi di sicurezza la scuola è vieta l'utilizzo questi sistemi.

- I sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica quindi, quando si invia un messaggio a più destinatari che non si conoscono tra loro, è necessario evitare che i destinatari possano vedere e conoscere i propri indirizzi di posta elettronica.
- 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.

## Art. 6 – Contenuti prodotti dagli utenti

- I contenuti pubblicati sulle applicazioni web hanno diversi livelli di visibilità (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 la pubblicazione di materiale all'interno di una community richiede l'utilizzo corretto delle funzioni necessarie all'attribuzione dei vari livelli di privacy.
- Dal momento che ciò che viene pubblicato su un Social Network è persistente e spesso non è facile da cancellare, se non impossibile, bisogna evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato.
- Quando si opera all'interno di un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto della community. Inoltre, è necessario conoscere gli strumenti per segnalare materiale e comportamenti non idonei.
- Se l'ambiente/contesto nel quale si intende pubblicare il proprio contributo prevede l'intervento di un moderatore assicurarsi che i contenuti oggetto di pubblicazione siano rispondenti alle regole richieste. Se non è visibile online, probabilmente non è idoneo.
- 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. Se il TAG riguarda una persona è opportuno contattarla preventivamente per ottenere il consenso a collegare l'identità della persona al contenuto.

## Art. 7 - Reati e violazioni della legge

Spesso il modo di operare in rete nasconde comportamenti che seppur apparentemente innocui possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali dalle conseguenze molto serie. Di seguito si riportano alcuni riferimenti legislativi specifici.

- ### Reati informatici

La legge 23 dicembre 1993, n. 547 Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, pubblicata su Gazzetta Ufficiale n.305 del 30-12-1993 ed entrata in vigore il 14-1-1994 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 sproteggere 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 o 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. È considerato reato anche quando l'informazione viene fraudolentemente carpita con "inganni" verbali e quando si prende conoscenza diretta di documenti cartacei ove tali dati sono stati riportati o osservando e memorizzando la "digitazione" di tali codici. - Si commette questo reato quando si carpiscono, anche involontariamente, i codici di accesso alla posta elettronica, al messenger o al profilo di amici e compagni.

- 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 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. o 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 on-line, accompagnato da informazioni non veritiere o ingiuriose: ciò potrebbe indurre altre persone a contattare la persona per le ragioni legate alle informazioni su questa fornite.

- Violazione dei diritti d'autore

La legge 22 aprile 1941, n. 633 sottolinea all'art. I 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.

## Art. 8 Prevenzione, rilevazione e gestione dei casi

### Prevenzione

I rischi che gli alunni possono correre a scuola nell'utilizzo delle TIC possono derivare da un uso non corretto del telefono cellulare personale o, ma solo in alcuni casi (es. connessione a server di posta elettronica accessibili da web) dei pc della scuola collegati alla rete. Attraverso strumenti personali (esempio smartphone dotati di connessione propria e/o particolari applicazioni) gli alunni potrebbero scaricare e spedire foto personali o di altri, video con contenuti non appropriati, accedere a siti non adatti ai minori o giocare con videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi.

### Le azioni previste di prevenzione nell'utilizzo delle TIC sono le seguenti:

- informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire;

- fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a);

- consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, finalizzati solo ad un uso esclusivamente didattico e comunque sotto la supervisione dell'insegnante,

- Se la condotta incauta dell'alunno consiste nel fare circolare immagini imbarazzanti, di natura sessuale, su internet, è necessario rimuoverle: contattare il service provider e se il materiale postato viola i termini e le condizioni d'uso del sito chiedere di rimuoverle.

### Rilevazione

- Contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso di strumenti personali o scolastici possono essere i seguenti:

- Contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi. Inoltre per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela. Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti). In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

## Art.9 - Operazioni non autorizzate

E' vietato, a studenti e docenti, installare programmi non autorizzati su tutte le postazioni informatiche della scuola. Qualora fosse necessario, solo ed esclusivamente per fini didattici, istallare software non in dotazione alla scuola, il docente direttamente interessato deve produrre apposita richiesta al dirigente scolastico specificando:

- Tipo di programma
- Utilizzo
- Eventuale costo
- Classi e modulo di programmazione interessate all'attività prevista con il programma richiesto

Solo dopo una accettazione con un apposito verbale da parte del team digitale si potrà procedere all'acquisto e/o all'istallazione del software