E-SAFETY POLICY

1. INTRODUZIONE

Finalità della e-safety policy

Il presente documento è volto a descrivere la linea di condotta dell'I.T.C.G. "Fermi" di Tivoli (RM) nei confronti dell'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (T.I.C.) nella didattica, in ambito scolastico ed extrascolastico, relativamente alle attività di studio domestico per lo svolgimento dei compiti assegnati dai docenti.

In particolare, la finalità precipua della scuola è quella di promuovere l'uso consapevole e critico da parte degli studenti delle tecnologie digitali e di Internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle T.I.C.

Ruoli e Responsabilità

Dirigente scolastico	Il ruolo del Dirigente scolastico include i seguenti compiti: ✓ garantire la sicurezza (tra cui la sicurezza on line) dei membri della comunità scolastica; ✓ garantire che tutti i docenti 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 T.I.C.; ✓ 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 T.I.C. a scuola.
Animatore digitale	Il ruolo dell'Animatore digitale include i seguenti compiti: ✓ stimolare la formazione interna all'istituzione nell'ambito del P.N.S.D. (Piano Nazionale della Scuola Digitale) e fornire consulenza ed 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 T.I.C. 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; ✓ assicurare che gli utenti possano accedere alla rete wi-fi della scuola solo tramite password applicate e regolarmente cambiate; ✓ coinvolgere la comunità scolastica (in primis docenti, studenti, genitori) nella partecipazione ad attività e progetti nell'ambito del P.N.S.D.
Direttore dei servizi generali e amministrativi	Il ruolo del Direttore dei servizi generali e amministrativi include i seguenti compiti: ✓ assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di esperti 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 (in particolare il sito web dell'istituto: http://www.fermitivoli.gov.it) all'interno della scuola e fra la scuola e le famiglie degli studenti per la notifica di circolari ed altri documenti del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle T.I.C. e di internet.

Docenti e personale educativo	Il ruolo del personale docente e del personale educativo include i seguenti compiti: ✓ informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle T.I.C. e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; ✓ garantire che le modalità di utilizzo corretto e sicuro delle T.I.C. e di Internet siano integrate nel curricolo di istituto e nelle attività didattico-educative delle classi; ✓ garantire che gli studenti comprendano e seguano le regole al fine di prevenire e contrastare l'utilizzo scorretto e pericoloso delle T.I.C. e di Internet; ✓ assicurare che gli studenti abbiano una buona comprensione delle opportunità di ricerca offerte dalle T.I.C. 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 studenti 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 T.I.C. e di tutti i dispositivi elettronici da parte degli studenti durante le lezioni ed ogni altra attività scolastica (ove consentito); ✓ nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli studenti a siti sicuri e adatti per il loro uso, controllare che le ricerche su Internet forniscano esclusivamente materiali didattici idonei; ✓ comunicare ai genitori difficoltà, bisogni o disagi espressi dagli studenti (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle T.I.C. e di Internet, 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 T.I.C.; ✓ segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli studenti in relazione all'utilizzo delle T.I.C. o di Internet, per l'adozione delle procedure previste dalle norme.
Studenti	Il ruolo degli studenti include i seguenti compiti: ✓ essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo delle T.I.C. e di Internet in conformità con quanto richiesto dai docenti; ✓ acquisire la consapevolezza delle potenzialità offerte dalle T.I.C. e dalla Rete per la ricerca di contenuti e materiali didattici ma anche della necessità di evitare il plagio e rispettare la normativa sul diritto d'autore; ✓ comprendere l'importanza di adottare buone pratiche di sicurezza on line quando si utilizzano le T.I.C. e la Rete per non correre rischi; ✓ rispettare la "netiquette" (le regole di buona educazione per la comunicazione online); ✓ esprimere domande, difficoltà o bisogno di aiuto nell'utilizzo delle T.I.C. o di Internet ai docenti e ai genitori.
Genitori	Il ruolo dei genitori degli studenti include i seguenti compiti: ✓ sostenere la linea di condotta della scuola adottata nei confronti

	dell'utilizzo delle T.I.C. nella didattica; ✓ seguire i propri figli nello studio a casa adottando i suggerimenti e le condizioni d'uso delle T.I.C. 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 T.I.C. o di Internet; ✓ stabilire delle regole per l'utilizzo del PC e tenere sotto controllo l'uso che i figli fanno di Internet e dei dispositivi elettronici (cellulare, smartphone, iPhone, tablet, iPad, ecc).

Condivisione e comunicazione della e-safety policy all'intera comunità scolastica

Condividere e comunicare la e-safety policy agli studenti:

- ✓ tutti gli studenti saranno informati che la Rete, l'uso di Internet e di tutti i dispositivi elettronici saranno controllati dai docenti ed utilizzati solo con la loro autorizzazione;
- ✓ l'istruzione degli studenti riguardo all'uso responsabile e sicuro di Internet precederà l'accesso alla rete;
- ✓ l'elenco delle regole per la sicurezza on-line sarà pubblicato nei laboratori con accesso a Internet;
- ✓ sarà molto importante educare gli studenti alla sicurezza in Rete, in particolare agli aspetti per i quali essi risultano più esposti o rispetto ai quali risultano più vulnerabili.

Condividere e comunicare la e-safety policy al personale:

- ✓ la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle T.I.C. e di Internet sarà discussa durante le riunioni degli OO.CC. e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web dell'istituto;
- ✓ per proteggere tutto il personale e gli studenti, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali;
- ✓ il personale docente sarà reso consapevole del fatto che il traffico in Internet potrà essere monitorato (si potrà risalire al singolo utente registrato);
- ✓ un'adeguata (in)formazione on line circa l'uso sicuro e responsabile di Internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web dell'istituto;
- ✓ il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle T.I.C. sarà supervisionato dagli assistenti tecnici e dall'Animatore digitale, che segnaleranno al D.S. e al D.S.G.A. eventuali problemi che dovessero richiedere acquisti o interventi di esperti esterni;
- ✓ l'Animatore digitale fornirà utili strumenti che il personale docente potrà utilizzare con gli studenti in classe;
- ✓ tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Condividere e comunicare la e-safety policy ai genitori:

- ✓ si attirerà l'attenzione dei genitori sulla sicurezza nell'uso delle T.I.C. e di Internet nel sito web della scuola;
- ✓ sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle T.I.C. e di Internet in occasione degli incontri scuola-famiglia e delle riunioni collegiali;
- ✓ l'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle T.I.C. e di Internet anche a casa;
- ✓ l'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi di siti web relativi a risorse utili, idonee ed educative per lo studio e per le attività da svolgere nel tempo libero, nonché sistemi di filtraggio;
- ✓ i genitori esperti potranno collaborare nelle attività di (in)formazione del personale e degli studenti.

Gestione delle infrazioni alla e-safety policy

Disciplina degli studenti

Le potenziali infrazioni in cui è possibile che gli studenti incorrano a scuola nell'utilizzo delle T.I.C. e di Internet sono prevedibilmente le seguenti:

- ✓ un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- ✓ l'invio incauto o senza permesso di foto o di altri dati personali (es. l'indirizzo di casa o il numero di telefono);
- ✓ la condivisione di immagini intime o troppo spinte;
- ✓ la comunicazione incauta e non autorizzata con sconosciuti;
- ✓ il collegamento a siti web non indicati dai docenti.

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati alla gravità del comportamento, quali:

- ✓ il richiamo verbale;
- ✓ il richiamo scritto con annotazione sul registro di classe;
- ✓ la convocazione dei genitori da parte dei docenti;
- ✓ la convocazione dei genitori da parte del Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli studenti della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle T.I.C. e di Internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle T.I.C. da parte degli studenti:

- ✓ un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- ✓ un utilizzo delle comunicazioni elettroniche con i genitori e gli studenti non compatibile con il ruolo professionale;
- ✓ un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- ✓ una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- ✓ una carente istruzione preventiva degli studenti sull'utilizzazione corretta e responsabile delle T.I.C. e di Internet;
- ✓ omissione di vigilanza degli studenti che può favorire un utilizzo non autorizzato delle T.I.C. e possibili incidenti;
- ✓ insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle T.I.C. per verificarne la conformità alle regole di sicurezza, compreso l'accesso a Internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive indagini. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo, gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

Alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle T.I.C. da parte degli studenti a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Le situazioni familiari meno favorevoli sono:

- ✓ la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- ✓ una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- ✓ una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare, dello smartphone o di altri dispositivi elettronici connessi alla Rete;
- ✓ un utilizzo del PC in comune con gli adulti che possono conservare in memoria materiali non idonei;
- ✓ un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli studenti possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

Monitoraggio dell'implementazione della e-safety policy e suo aggiornamento

Il monitoraggio dell'implementazione della e-safety policy e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale e dai docenti delle classi, tramite questionari o conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno scolastico, in relazione all'uso sicuro e responsabile delle T.I.C. e di Internet. Il monitoraggio sarà rivolto anche ai docenti, al fine di valutare l'impatto della e-safety policy e la necessità di eventuali miglioramenti. L'aggiornamento della e-safety policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dagli Organi Collegiali, a seconda degli aspetti considerati.

Integrazione della e-safety policy con il Regolamento d'Istituto

Si riporta l'articolo del Regolamento di Istituto integrato con la potica E-Safety:

USO CELLULARI ED ALTRI DISPOSITIVI ELETTRONICI

Alla luce della Direttiva Ministeriale del 15 marzo 2007, è vietato l'uso del telefono cellulare e di ogni altro dispositivo elettronico, rappresentando un elemento di distrazione sia per chi lo usa che per i compagni, oltre che una grave mancanza di rispetto per il docente; pertanto, subito dopo l'ingresso in classe, dovrà essere depositato in apposito contenitore presente in classe.

Durante il cambio orario tra docenti, il cellulare sarà prelevato dal proprietario per poi essere nuovamente depositato, dallo stesso, all'inizio della successiva ora.

Durante lo svolgimento delle attività didattiche, eventuali esigenze di comunicazione tra gli studenti e le famiglie, dettate da ragioni di particolare urgenza o gravità, potranno sempre essere soddisfatte, previa autorizzazione del docente.

La scuola continuerà, in ogni caso, a garantire, come è sempre avvenuto, la possibilità di una comunicazione reciproca tra le famiglie ed i propri figli, per gravi ed urgenti motivi, mediante gli uffici di presidenza e di segreteria amministrativa.

A discrezione del docente, è consentito l'uso di dispositivi elettronici solo per fini didattici.

La violazione di tale obbligo costituisce infrazione disciplinare, sanzionata in base a quanto previsto dalla tabella A, oltre che configurare, in casi estremi, violazione di legge (Codice della Privacy D. Lgs. 196/2003 e dell'art. 10 del Codice Civile).

Il divieto di utilizzare telefoni cellulari durante lo svolgimento di attività di insegnamento – apprendimento opera anche nei confronti del personale docente (Circolare n. 362 del 25 agosto 1998).

Si riporta altresì lo stralcio della tabella che riguarda le infrazioni disciplinari non gravi – individuali:

TABELLA INFRAZIONI DISCIPLINARI NON GRAVI - INDIVIDUALI				
DOVERI (art.3 DPR 24 giugno 1998 n. 249)	**INFRAZIONI**	**QUANDO SCATTA LA SANZIONE**	**SANZIONI**	**COME SI PROCEDE**
RISPETTO PER GLI ALTRI E COMPORTAMENTO COERENTE CON I PRINCIPI DELLA COMUNITA' SCOLASTICA	*Uso improprio del cellulare o altri apparecchi elettronici*	*Dopo ripetute violazioni*	• *Ammonizione verbale o scritta* • *Valutazione del comportamento* • *Esclusione dalla partecipazione ad iniziative extra didattiche del gruppo classe (visione film, teatro, visite aziendali, visite e viaggi di istruzione, ecc.)* *La sanzione che comporta l'esclusione dalla partecipazione ad iniziative extra didattiche del gruppo classe è adottata anche tenendo conto delle caratteristiche personali e dei comportamenti pregressi dello studente e al fine di garantire la sicurezza e un'adeguata vigilanza sugli studenti che non può prescindere dalla valutazione del grado di maturazione di ciascuno studente.*	• *Applicazione da parte di un docente o del Dirigente scolastico o del Consiglio di classe (ammonizione).* • *Esclusione dalla partecipazione ad iniziative extra didattiche del gruppo classe (Consiglio di classe o coordinatore di classe o Dirigente scolastico).* • *Voto di comportamento da parte del Consiglio di classe in sede di valutazione.*

2. FORMAZIONE E CURRICOLO

Competenze digitali per gli studenti

Il 18 dicembre 2006 la Gazzetta Ufficiale dell'Unione Europea ha pubblicato la Raccomandazione del Parlamento Europeo e del Consiglio d'Europa relativa alle competenze chiave per l'apprendimento permanente. Il documento definisce otto macrocompetenze ed invita gli Stati membri a svilupparne l'offerta nell'ambito delle loro strategie di apprendimento permanente (*life-long learning*).
Le competenze chiave sono quelle di cui tutti hanno bisogno per la realizzazione e lo sviluppo personali, la cittadinanza attiva, l'inclusione sociale e l'occupazione.

Tra le competenze chiave rientra la competenza digitale che *consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per*

reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet.

CONOSCENZE, ABILITÀ E ATTITUDINI ESSENZIALI LEGATE A QUESTA COMPETENZA	
Conoscenze	*La competenza digitale presuppone una solida consapevolezza e conoscenza della natura, del ruolo e delle opportunità delle TSI nel quotidiano: nella vita privata e sociale come anche al lavoro. In ciò rientrano le principali applicazioni informatiche come trattamento di testi, fogli elettronici, banche dati, memorizzazione e gestione delle informazioni oltre a una consapevolezza delle opportunità e dei potenziali rischi di Internet e della comunicazione tramite i supporti elettronici (e-mail, strumenti della rete) per il lavoro, il tempo libero, la condivisione di informazioni e le reti collaborative, l'apprendimento e la ricerca. Le persone dovrebbero anche essere consapevoli di come le TSI possono coadiuvare la creatività e l'innovazione e rendersi conto delle problematiche legate alla validità e all'affidabilità delle informazioni disponibili e dei principi giuridici ed etici che si pongono nell'uso interattivo delle TSI.*
Abilità	*Le abilità necessarie comprendono: la capacità di cercare, raccogliere e trattare le informazioni e di usarle in modo critico e sistematico, accertandone la pertinenza e distinguendo il reale dal virtuale pur riconoscendone le correlazioni. Le persone dovrebbero anche essere capaci di usare strumenti per produrre, presentare e comprendere informazioni complesse ed essere in grado di accedere ai servizi basati su Internet, farvi ricerche e usarli. Le persone dovrebbero anche essere capaci di usare le TSI a sostegno del pensiero critico, della creatività e dell'innovazione.*
Attitudini essenziali	*L'uso delle TSI comporta un'attitudine critica e riflessiva nei confronti delle informazioni disponibili e un uso responsabile dei mezzi di comunicazione interattivi. Anche un interesse a impegnarsi in comunità e reti a fini culturali, sociali e/o professionali serve a rafforzare tale competenza.*

Fonte: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32006H0962

TUTTE le discipline (generali e di indirizzo) che si insegnano/apprendono nei tre indirizzi del nostro istituto (servizi socio-sanitari, servizi commerciali/promozione commerciale e pubblicitaria, liceo artistico - indirizzo grafica) possono concorrere alla formazione dello studente "digitale", soprattutto grazie alla presenza di numerosi laboratori nelle due sedi del nostro istituto (di informatica, di grafica, di lingue, di scienze, di metodologie operative), nonché di aule multimediali dotate di LIM.

Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire i pericoli. In questo senso, tutti gli insegnanti e tutte le discipline sono coinvolti nello sviluppo di tale competenza.

Formazione dei docenti sull'utilizzo e l'integrazione delle T.I.C. nella didattica

È importante sottolineare il fatto che il personale scolastico del nostro istituto è disponibile ad aggiornarsi per utilizzare al meglio le T.I.C. in ambito didattico o amministrativo.
Il percorso lungo e complesso della formazione specifica dei docenti sull'utilizzo delle T.I.C. nella didattica può prevedere occasioni di autoaggiornamento, di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo; può comprendere altresì la fruizione dei materiali messi a disposizione dall'Animatore digitale e corsi di aggiornamento online.

Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche gli studenti.

Sensibilizzazione delle famiglie

Per sensibilizzare le famiglie all'uso consapevole delle T.I.C. e della Rete, promuovendo la conoscenza delle numerose situazioni di rischio online, si potranno organizzare incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone, *chat line* (es. Messenger) o *social network* (es. Facebook) più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

Il cyberbullismo è mobbing in Internet, infatti, per designarlo si usano anche i termini cybermobbing e internet mobbing. Viene messo in atto mediante l'uso dei media digitali e consiste nell'invio ripetuto di messaggi offensivi tramite sms, in chat o su Facebook per molestare una persona per un lungo periodo.

Gli autori, i cosiddetti «bulli» o il cosiddetto «branco», sono spesso persone che la vittima ha conosciuto a scuola, nel quartiere o in un'associazione. Offendono, minacciano o ricattano le loro vittime direttamente o facendo pressione psicologica su di loro, le diffamano, le mettono alla gogna e diffondono dicerie sul loro conto. Chi ne è vittima può subire conseguenze molto gravi, come la perdita della fiducia in se stesso, stati di ansia e depressione.

Il confine tra un comportamento che resta scherzoso e uno che è percepito come offensivo non è così netto. Il cyberbullismo inizia laddove un individuo si sente importunato, molestato e offeso. Raramente i giovani si rendono conto delle conseguenze delle loro azioni nel momento in cui mettono in rete immagini offensive o le inviano agli amici; spesso lo fanno solo per scherzo. Tuttavia, può trattarsi anche di atti mirati a rovinare una persona.
Fonte: http://www.giovaniemedia.ch/it/opportunita-e-rischi/rischi/cyberbullismo.html

L'istituto si impegna alla diffusione delle informazioni e delle procedure contenute nel presente documento per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati ad un utilizzo non corretto di Internet.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE T.I.C. DELLA SCUOLA.

Accesso a Internet

L'accesso a Internet a scopi didattici è possibile nei laboratori multimediali, dove c'è una postazione di lavoro per il docente (server) e numerose postazioni in Rete per gli studenti (client). Tutti gli utenti dell'istituto (studenti, docenti, personale A.T.A.) devono inserire le proprie credenziali per utilizzare i PC ed accedere alla Rete. L'accesso è comunque filtrato per tutti: il server impedisce il collegamento a siti appartenenti a *black list* e consente il collegamento solo a siti idonei all'attività didattica.

I docenti annotano su un registro la data, l'orario di utilizzo del laboratorio, la classe e comunicano tempestivamente agli assistenti tecnici eventuali problemi riscontrati durante la lezione. Tutti possono effettuare il backup dei file elaborati su supporti rimovibili personali (es. chiavette USB).

E-mail

Tutto il personale scolastico possiede un account per l'accesso al sito istituzionale.

Sito web della scuola

La scuola è dotata di un proprio sito web aggiornato con l'adeguamento ai requisiti di accessibilità dei siti delle PA. Oltre ad una nuova veste grafica sono stati migliorati alcuni servizi e ne sono stati aggiunti altri. Una ulteriore novità del sito è quella che riguarda la necessità di registrarsi sia per le famiglie sia per i docenti. La registrazione permetterà di fruire dei contenuti e dei servizi previsti per gli utenti registrati (Programmi svolti, Programmazioni didattiche, Invio Moduli OnLine, allegati alle circolari etc.). Si ricorda inoltre che con la registrazione al sito si viene automaticamente iscritti alla newsletter dalla quale, a seconda della lista di appartenenza (famiglie, docenti, ata) verranno inviate esclusivamente comunicazioni riguardanti la vita scolastica. La gestione e l'aggiornamento è curato dal webmaster, Prof. Paolo De Falco, contattabile all'indirizzo postmaster@fermitivoli.gov.it.

Social network

L'istituzione scolastica ha realizzato una pagina Facebook "Istituto E. Fermi (link: https:// www.facebook.com/ITCG-Enrico-Fermi), con finalità informativa e pubblicitaria.

Protezione dei dati personali

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi. Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

4. STRUMENTAZIONE PERSONALE

Per gli studenti: gestione degli strumenti personali – cellulari, tablet ecc.

È consentito l'uso di strumenti elettronici personali (smartphone, tablet, ecc.) esclusivamente per lo svolgimento di attività didattiche e solo se autorizzati dai docenti.

Per i docenti: gestione degli strumenti personali – cellulari, tablet ecc.

Durante le ore delle lezioni non è consentito l'utilizzo del proprio cellulare o smartphone per comunicazioni personali. È consentito l'uso dei dispositivi elettronici personali (tablet, iPad, notebook) per attività didattiche e funzionali all'insegnamento.

Per il personale A.T.A.: gestione degli strumenti personali – cellulari, tablet ecc.

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per urgenti comunicazioni personali.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Prevenzione

Rischi

I rischi effettivi che si possono correre a scuola nell'utilizzo delle T.I.C. da parte degli studenti derivano da un uso non corretto del telefono cellulare personale, dello smartphone e dei PC della scuola collegati alla Rete.

Il telefono cellulare o lo smartphone non sono ritenuti strumenti indispensabili in ambito scolastico. Eludendo la sorveglianza degli insegnanti, attraverso i propri telefoni cellulari, smartphone/iPhone, dotati di particolari applicazioni e di collegamento a Internet, oltre che parlare e scrivere messaggi con i familiari o gli amici, gli studenti potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a Internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e

minacciosi. Eludendo sempre la vigilanza dei docenti, gli studenti potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei PC e con un accesso non controllato a Internet.

Azioni

Si prevedono le seguenti azioni di prevenzione nell'utilizzo delle T.I.C.:

- ✓ 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, video, immagini, testi e disegni relativi al proprio/a figlio/a);
- ✓ non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;
- ✓ consentire l'utilizzo del cellulare solo in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione del docente, che si accerta preventivamente dell'identità dell'interlocutore;
- ✓ utilizzare filtri, software che impediscono il collegamento ai siti web non idonei (*black list*);
- ✓ centralizzare il blocco dei siti web sul server del docente, utilizzando software che possono bloccare l'accesso ai siti Internet semplicemente esaminando le varie richieste di connessione provenienti dai client collegati in rete locale, in modo tale che anche indipendentemente dal browser in uso su ciascuna macchina, il software sia capace di intercettare le richieste di collegamento e rigettare quelle che non rispettano le regole imposte dall'amministratore.

Le azioni di contenimento degli incidenti previste sono le seguenti:

- ✓ se la condotta incauta dello studente 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;
- ✓ se lo studente viene infastidito od offeso, suggerirgli di modificare i dettagli del proprio profilo sistemandolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messengers, siti social network, Skype, ecc.), o suggerirgli di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici con i quali regolarmente chatta, di inserire il compagno o la persona che offende, per quanto riguarda l'e-mail, tra gli indesiderati;
- ✓ consigliare di cambiare il proprio indirizzo e-mail, contattando l'e-mail provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati (es. Calls Blacklist) o, se necessario, cambiare il numero di cellulare contattando l'operatore telefonico;
- ✓ fare cancellare il materiale offensivo dal cellulare, facendo intervenire i genitori, e chiedere agli studenti di indicare a chi e dove lo hanno spedito per farlo fare anche gli altri, e conservare una copia di detto materiale se necessario per ulteriori indagini;
- ✓ contattare la polizia se si ritiene che il materiale offensivo sia illegale. In caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi elettronici ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò è reato per chiunque.

Rilevazione

Che cosa segnalare

Gli studenti possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli studenti sui rischi delle comunicazioni on line, i minori possono riferire di fatti o eventi personali o altrui che "allertano" il docente.

Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dallo studente, può essere presentata da un reclamo dei genitori, può essere notata dal docente che si accorge dell'infrazione in corso. Mentre il docente è autorizzato a controllare le strumentazioni della scuola, per controllare l'uso del telefono cellulare/dello smartphone di uno studente si rivolge al genitore.

I contenuti "pericolosi" comunicati/ricevuti a/da altri, caricati/scaricati in Rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola attualmente dagli studenti (il cellulare, lo smartphone, l'iPhone personale e il PC collegato a Internet) 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, malware, 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.

Come segnalare: quali strumenti e a chi.

Per il cellulare/lo smartphone ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine/video, conservando così il numero del mittente.

I docenti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui PC della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto.

Qualora ci si dovesse accorgere che lo studente, usando il computer, si sta servendo di un servizio di messaggeria istantanea, programma che permette di chattare in linea tramite testo, il docente può copiare, incollare e stampare la conversazione. Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting sites ed altri siti web, il docente può conservare il link, stampare la pagina o salvare la schermata su un documento Word. Per le e-mail si può stampare la mail o conservare l'intero messaggio, compresa l'intestazione del mittente.

Conservare la prova è utile per far conoscere l'accaduto, in base alla gravità, ai genitori degli studenti, al Dirigente scolastico, alla polizia.

Qualora non si disponga di prove, ma solo delle testimonianze dello studente, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, anche alla polizia.

In particolare la segnalazione viene fatta ad entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro studente.

Per le segnalazioni di fatti rilevanti sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

1. annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
2. convocazione scritta e colloquio con i genitori degli studenti, da parte dei docenti;
3. relazione scritta al Dirigente scolastico.

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 studenti 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 tutti i dati che consentono l'identificazione della 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.

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

Gestione dei casi di "immaturità"

Può sembrare naturale allo studente fornire i propri dati sui siti allestiti in modo tale da attrarre la sua attenzione, con giochi e animazioni, personaggi simpatici e divertenti, che richiedono una procedura di registrazione.

Curiosità, manifestazioni di reciproco interesse tra pari, idee e fantasie sulla sessualità sono espressione da una parte del progressivo sviluppo socio-affettivo dello studente e dall'altra dei molteplici messaggi espliciti che gli giungono quotidianamente attraverso i media (televisione, DVD, Internet, giornali, riviste, ecc.), i discorsi dei coetanei o degli adulti.

I comportamenti cosiddetti "quasi aggressivi", che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro "per gioco", effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l'alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell'autonomia dall'adulto e pertanto luogo di "complicità" e di piccole "trasgressioni", di scambi "confidenziali"condivisi fra gli amici nella Rete o con il cellulare.

Detti comportamenti, che finiscono per arrivare all'attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

Gestione dei casi di "prepotenza" o "prevaricazione"

I comportamenti definibili "bullismo" possono esprimersi nelle forme più varie e non sono sempre identificabili a priori, se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali fra i ragazzi sono la costanza nel tempo e la ripetitività, l'asimmetria (disuguaglianza di forza e di potere), il disagio della/e vittima/e.

Il bullismo si esplica infatti con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto, ma in genere da un gruppo.

Nel caso particolare del cyberbullismo, le molestie sono attuate attraverso dispositivi tecnologici: invio di sms, messaggi in chat, e-mail offensive o minacciose; diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing list o nelle chatline; pubblicazione nel cyberspazio di foto o filmati che ritraggono atti di prepotenza o denigrazione subiti dalla vittima.

In particolare, il bullismo può nascere anche dall'esasperazione di conflitti presenti nel contesto scolastico. Il conflitto, presente in ogni normale interazione, è da considerarsi come un campanello d'allarme e può degenerare in forme patologiche quando non lo si riconosce e gestisce in un'ottica evolutiva dei rapporti, di negoziazione e risoluzione. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull'ambiente (alterazione del clima del gruppo-classe).

Per prevenire e affrontare il bullismo, dunque, i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli studenti.

L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli studenti, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno.

Gli interventi mirati sul gruppo-classe sono gestiti in collaborazione dal team dei docenti della classe e d'intesa con le famiglie - ad esempio con percorsi di mediazione volta alla gestione positiva del

conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, con le strategie del problem-solving.

Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.

Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire negli studenti un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza"ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani", per rendere consapevoli gli studenti del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on line deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale.

Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto psicologico gratuito se attivo presso la scuola. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

Gestione degli "abusi sessuali"

"In generale si parla di abuso sessuale sui minori quando un minore viene coinvolto in un atto sessuale. Ciò è caratterizzato dal fatto che il minore non comprende del tutto tale atto, non è informato e quindi non è in grado di acconsentire, oppure sulla base del suo livello di sviluppo non è ancora pronto per tale atto e non può dare il proprio consenso".

Lo spettro delle forme di abuso e di violenza è diventato ancora più ampio e subdolo in seguito alle possibilità offerte dai nuovi mezzi di comunicazione come Internet, il cellulare o altri dispositivi tecnologici, e il loro utilizzo sempre più diffuso non fa che acuire il problema. Internet, infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile.

Succede sempre più frequentemente che un adulto prenda contatto con i minori nei forum o nelle chat su Internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i minori a spogliarsi davanti alla webcam oppure a inviare una fotografia che li ritrae nudi tramite Internet o sul cellulare, per poi ricattarli e costringerli a non rivelare gli abusi. Spesso l'adulto finge di essere minorenne.

La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte dei docenti o del Dirigente scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, socio-psicologico e giudiziario.

Il compito della scuola non è comunque solo quello di "segnalare", ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il minore a riprendere una crescita serena.

A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

ALLEGATI

DICHIARAZIONE LIBERATORIA PER L'ACCESSO AD INTERNET NELLA RETE WI-FI DI ISTITUTO, PER L'UTILIZZO DEI DISPOSITIVI ELETTRONICI, PER LA PUBBLICAZIONE DI NOMI, ELABORATI SCRITTI, GRAFICI, FOTOGRAFICI, AUDIOVISIVI

AL DIRIGENTE SCOLASTICO

DELL'I.T.C.G. "FERMI"

VIA ACQUAREGNA, 112

TIVOLI (RM)

Il/La sottoscritto/a _____, in qualità di genitore/tutore dell'alunno/a_____, iscritto/a alla classe _____ sez. _____ indirizzo _____ dell'I.T.C.G. "Fermi" di Tivoli:

DICHIARA

- di essere a conoscenza della e-safety policy (politica di sicurezza in Rete) adottata dall'I.T.C. G. FERMI" e pubblicata sul sito web istituzionale (link: https://www.fermitivoli.gov.it/
- di essere consapevole delle implicazioni di responsabilità personale derivanti dall'accesso a Internet, dall'uso di cellulare, smartphone/iPhone e di altri dispositivi elettronici (tablet, iPad, notebook, ecc.) e dagli eventuali abusi.

In particolare, si impegna a che il/la figlio/a:

- non scarichi/duplichi/distribuisca software o altri contenuti protetti da diritto d'autore;
- non acceda a siti web o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola (ad esempio, siti con contenuto violento, pedo-pornografico, razzista, ecc.);
- non diffonda virus e/o malware all'interno della Rete e a dare immediato avviso all'Amministrazione della Rete di comportamenti anomali o di infezioni riconosciute;
- non utilizzi cellulare, smartphone/iPhone o altri dispositivi elettronici personali a scuola per scopi non didattici e soprattutto senza l'autorizzazione dei docenti;
- partecipi con impegno agli interventi educativi della scuola sulle modalità di utilizzo sicuro e consentito dei dispositivi elettronici e di Internet.

Il/La sottoscritto/a

AUTORIZZA

l'I.T.C.G. "E. Fermi" di Tivoli (RM) a realizzare e ad utilizzare, a scopo didattico e/o di documentazione e/o di informazione e senza fini di lucro, fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome, la voce, gli elaborati (scritti, disegni, ecc.) del/la proprio/a figlio/a anche, se del caso, mediante riduzioni e/ o adattamenti.

DICHIARA

- di essere informato/a che detto materiale potrà essere utilizzato per documentare e divulgare le attività didattiche tramite il sito web di Istituto, pubblicazioni, CD-ROM, mostre, seminari, convegni e altre iniziative promosse dalla scuola anche in collaborazione con altri soggetti;
- di non aver nulla a pretendere in ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato;
- che le suddette autorizzazioni/dichiarazioni hanno validità per l'intero ciclo della scuola secondaria di secondo grado, salvo eventuale successiva revoca.

Luogo e data: _____

Firma leggibile del genitore/tutore _____

Firma leggibile dello studente/della studentessa _____

MODULO DI RICHIESTA DI CREDENZIALI DI AUTENTICAZIONE/DI ACCESSO AD INTERNET

NELLA RETE DI ISTITUTO E DI UTILIZZO DEI DISPOSITIVI ELETTRONICI

AL DIRIGENTE SCOLASTICO

DELL'I.T.C.G. "FERMI"

VIA ACQUAREGNA, 112

TIVOLI (RM)

Il/La sottoscritto/a _____, in qualità di docente/personale ATA (cancellare la voce che non interessa) in servizio presso I.T.C.G. "E. Fermi" di Tivoli (RM) chiede il rilascio delle credenziali di autenticazione/l'accesso ad Internet nella rete di Istituto.

DICHIARA

- di essere a conoscenza della e-safety policy (politica di sicurezza in Rete) adottata dall'I.T.C.G. "E. Fermi" e pubblicata sul sito web istituzionale link: https://www.fermitivoli.gov.it/
- di essere consapevole delle implicazioni di responsabilità personale derivanti dall'accesso a Internet, dall'uso di cellulare, smartphone/iPhone e di altri dispositivi elettronici (tablet, iPad, notebook, ecc.) e dagli eventuali abusi.

In particolare si impegna a:

- non scaricare/duplicare/distribuire software o altri contenuti protetti da diritto d'autore;
- non accedere a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola (ad esempio, siti con contenuto violento, pedo-pornografico, razzista, etc…);
- non collegarsi ad Internet per scopi commerciali o di profitto personale e per attività illegali;
- non diffondere virus e malware all'interno della Rete e a dare immediato avviso all'Amministrazione della Rete di comportamenti anomali o di infezioni riconosciute;
- conservare le credenziali di accesso alla Rete in modo scrupoloso, non comunicandole ad altre persone. È consapevole che l'accesso attraverso l'autenticazione trasferisce direttamente la responsabilità degli atti commessi durante la navigazione all'intestatario delle credenziali stesse.

Dichiara di essere consapevole che:

- l'autorizzazione all'uso della rete di Istituto potrà venire revocata (cancellazione dell'utente) in qualsiasi momento per cause tecniche o per motivazioni legate all'uso improprio o alla violazione delle norme di comportamento;
- l'utilizzo dei dispositivi elettronici e della rete della scuola deve essere utilizzata per attività di servizio o funzionali alle stesse;
- l'utilizzo della rete per l'assunzione di impegni o responsabilità per conto della scuola deve essere autorizzata dal Dirigente scolastico, legale rappresentante dell'istituzione nonché legittimo titolare dell'utenza;
- l'utilizzo del cellulare e di altri dispositivi elettronici personali a scuola deve avvenire nei limiti consentiti dalla legge e dai regolamenti dell'istituzione scolastica, in situazioni di necessità ed urgenza o per ragioni di servizio;
- ci si deve rivolgere per la necessaria assistenza alla connessione o al funzionamento dei dispositivi contattando l'Animatore digitale, i referenti dei laboratori di informatica o gli uffici di segreteria, evitando tentativi incerti di ripristino o di modificazione delle impostazioni.

Luogo e data: _____

Firma leggibile: _____

PROCEDURE OPERATIVE PER LA RILEVAZIONE, IL MONITORAGGIO E LA GESTIONE DELLE SEGNALAZIONI

CYBERBULLISMO: alcuni campanelli di allarme

Gli atti di bullismo avvengono prevalentemente entro o nei dintorni del contesto scolastico, tuttavia in misura crescente le prepotenze vengono riportate nel contesto virtuale di Internet. In queste situazioni si parla di *cyberbullying* che si manifesta attraverso:

- ✓ invio di sms, mms, e-mail offensivi/e o di minaccia;
- ✓ diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle *mailing-list* o nelle *chat-line*;
- ✓ pubblicazione nel *cyberspazio* di foto o filmati che ritraggono atti di prepotenza o denigrazione subiti dalla vittima.

La rilevazione diretta degli indicatori da parte degli insegnanti o indiretta, sulla base di quanto riferito dagli studenti o dai genitori, deve affinarsi con l'osservazione delle relazioni interpersonali e delle possibili dinamiche conflittuali sottostanti presenti nel contesto classe, al fine di verificare l'entità e la natura del fenomeno e dare avvio al programma di intervento.

A chi segnalare:

L'attuazione del programma di intervento si basa prevalentemente sull'impiego delle risorse umane già presenti e disponibili: docenti e altro personale scolastico, studenti e genitori. Non serve, se non in casi particolarmente gravi, l'opera di psicologi, assistenti sociali, o altri specialisti a cui orientare la famiglia. L'elemento fondamentale per una buona riuscita del programma è infatti la corretta ristrutturazione del contesto relazionale degli studenti.

ABUSI SESSUALI: alcuni campanelli di allarme

Internet ha ampliato le possibilità di abuso sessuale dei minori. Infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile (pedopornografia) in cui le vittime sono appunto i minori. Inoltre succede che un adulto prenda contatto con dei bambini nei forum o nelle chat su internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i bambini a spogliarsi davanti alla webcam oppure a inviare una fotografia che li ritrae nudi tramite Internet o sul cellulare.

L'osservazione della presenza dei suddetti indicatori da parte degli insegnanti deve essere attenta e pronta alla segnalazione.

A chi segnalare:

In particolare nel caso in cui ci si dovesse imbattere in materiale pedopornografico (cioè contenuti foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali), è necessario "Innanzitutto evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto. Ciò è reato per chiunque. Nel venire a conoscenza di materiali di questo tipo è importante contribuire alla loro eliminazione: basta inserire le informazioni richieste sugli appositi moduli online, disponibili ai siti www.stop-it.it e http://www.azzurro.it/it/clicca-e-segnala" ovvero collegandosi al sito della polizia postale https://www.commissariatodips.it, dove è possibile sia segnalare che denunciare. In alternativa, è possibile recarsi nella sede più vicina della polizia giudiziaria. Ciò consente di operare con la massima tempestività. Non operare in modo isolato, ma confrontarsi con i colleghi di classe e il Dirigente Scolastico.

PROCEDURE OPERATIVE PER LA GESTIONE DEI CASI

LINEE GUIDA PER GLI STUDENTI

- ✓ Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere e caratteri speciali.
- ✓ Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola.
- ✓ Non inviare a nessuno fotografie tue o di tuoi amici.
- ✓ Prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso.
- ✓ Chiedi sempre al tuo docente a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet.
- ✓ Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola.
- ✓ Quando sei connessi alla rete RISPETTA SEMPRE GLI ALTRI: ciò che per te è un gioco può rivelarsi offensivo per qualcun altro.
- ✓ Non rispondere alle offese ed agli insulti.
- ✓ Blocca i bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli.
- ✓ Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto.
- ✓ Se ricevi materiale offensivo (email, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo.
- ✓ Rifletti prima di inviare: ricordati che tutto ciò che invii su Internet diviene pubblico e rimane per SEMPRE.
- ✓ Riferisci al tuo docente o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo docente o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet.
- ✓ Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo docente o ai tuoi genitori.
- ✓ Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.
- ✓ Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo docente prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa.
- ✓ Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo docente o dei tuoi genitori.
- ✓ Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo docente o dei tuoi genitori.

LINEE GUIDA PER I DOCENTI

- ✓ Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune.
- ✓ Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali.
- ✓ Discutete con gli studenti della e-safety policy della scuola, di utilizzo consentito della Rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet.
- ✓ Fornite chiare indicazioni sull'utilizzo di Internet, ed eventualmente anche la posta elettronica, ed informateli che le navigazioni saranno monitorate.
- ✓ Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata).
- ✓ Ricordate agli alunni che la violazione consapevole della e-safety policy della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo.
- ✓ Adottate provvedimenti "disciplinari", proporzionati all'età e alla gravità del comportamento.
- ✓ Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione

dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

- ✓ Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi (sportello di ascolto psicologico gratuito attualmente attivo presso la scuola, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).
- ✓ Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indizzo e-mail, ecc.
- ✓ Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro.
- ✓ In caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come Internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

1) Consigli generali

- ✓ Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia.
- ✓ Evitate di lasciare le e-mail o file personali sui computer di uso comune.
- ✓ Concordate con i vostri figli le regole: quando si può usare Internet e per quanto tempo.
- ✓ Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici.
- ✓ Aumentate il filtro del "parental control" attraverso la sezione sicurezza in internet dal pannello di controllo.
- ✓ Attivate il firewall (protezione contro malware) e antivirus.
- ✓ Mostratevi coinvolti: chiedete ai vostri figli di mostrarvi come funziona Internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare col docente.
- ✓ Incoraggiate le attività on line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo.
- ✓ Partecipate alle esperienze on line: navigate insieme ai vostri figli, incontrate amici on line, discutete gli eventuali problemi che si presentano.
- ✓ Comunicate elettronicamente con i vostri figli: inviate, frequentemente, e-mail, Instant Message.
- ✓ Spiegate ai vostri figli che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone.
- ✓ Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia).
- ✓ Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus.
- ✓ Raccomandate di non scaricare file da siti sconosciuti.
- ✓ Incoraggiate i vostri figli a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate.
- ✓ Discutete nei dettagli le conseguenze che potranno esserci se i vostri figli visitano deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie.
- ✓ Spiegate ai vostri figli che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati a nessuno.
- ✓ Spiegate ai vostri figli che non tutti in Internet sono chi realmente dichiarano di essere; di conseguenza i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima.
- ✓ Il modo migliore per proteggere i vostri figli è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

2) Consigli in base all'età (14-18 anni):

Verificate i profili dei vostri figli e dei loro amici, nei siti cerca persona, informandoli dei vostri periodici controlli. Ricordati che in questa fascia di età aumentano le ricerche di materiale sessuale ed i rischi di seduzioni sessuali on line da parte di cyberpredatori adulti: condividete con i vostri figli le procedure

per navigare in sicurezza ed evitare on line ed off line brutti incontri. Confrontatevi con i vostri figli su tutti questi rischi e se protestano per il controllo, ribadite che è un dovere dei genitori supervisionare e monitorare l'uso di internet. Stringete un accordo: se i vostri figli dimostrano di avere compreso i rischi e di sapere e volere usare internet in modo sicuro, diminuite la supervisione. Il computer deve rimanere in salone o in una stanza accessibile a tutta la famiglia e non nella camera dei vostri figli ALMENO fino ai 16 anni.

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

Non vi sono protocolli siglati ma ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo da parte dell'Ente Locale, del Consultorio familiare e del Comando dei Carabinieri.