Scuola Secondaria Statale di 1° grado

ISTITUTO COMPRENSIVO

"Filippo Traina"

POLICY DI E-SAFETY

A.S.2015/2016

1.Introduzione

- Scopo della Policy.

Il presente documento, realizzato in occasione del progetto SIC II (Safer Internet Centre) Generazioni Connesse, promosso dal MIUR in collaborazione con la comunità europea, mira a descrivere la linea di condotta dell'Istituto "Filippo Traina" di Vittoria nei confronti dell'utilizzo delle tecnologie dell'informazione e delle comunicazioni nella didattica, in ambito scolastico ed extrascolastico, nonché a educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di internet.

Nello specifico il documento mira a promuovere un uso critico da parte degli alunni delle tecnologie digitali e di internet; far acquisire loro corrette norme comportamentali, procedure e competenze per l'utilizzo delle TAC "Tecnologie Apprendimento Conoscenza", prevenire, rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.

- Ruoli e Responsabilità

Il Dirigente scolastico ha il compito di

• Garantire la sicurezza (tra cui la sicurezza on line) di tutti i membri della comunità scolastica.

• Garantire che tutti gli insegnanti ricevano una formazione adeguata per un utilizzo positivo e responsabile delle TAC.

• 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 TAC a scuola.

L'Animatore digitale ha il compito di:

• Stimolare la formazione interna all'istituzione sui temi del PNSD (Piano Nazionale Scuola Digitale) e fornire consulenza e informazioni al personale della scuola, agli alunni e alle loro famiglie 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.

• Individuare soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.

• Coinvolgere il più possibile tutta la comunità scolastica nella partecipazione ad attività e progetti attinenti il PNSD.

Il Direttore dei servizi generali ha il compito di:

• Garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a attacchi esterni dannosi o malevoli.

• Assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente modificate, e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali;

• Garantire il funzionamento dei diversi canali di comunicazione tra l'Istituzione scolastica e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Il docente ha il compito di:

• Informarsi/formarsi 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 gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TAC e di internet.

• Controllare l'uso delle tecnologie digitali (quali ad esempio ed a titolo non esaustivo, dispositivi mobili, macchine fotografiche e in generale strumenti di registrazione audio/video ecc.) da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito).

• Guidare le ricerche degli alunni su Internet, suggerendo siti controllati e verificati, adatti per l'uso didattico.

• Segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo 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 TAC.

• Segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola riguardante gli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle proc

dure previste dalle norme.

L'alunno ha il compito di:

• Essere responsabile nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti.

• 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 (*Netiquette*).

• Richiedere, se necessario, un aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Il genitore ha il compito di:

• Sostenere la linea di condotta adottata dalla scuola nei confronti dell'utilizzo delle TAC nella didattica.

• Seguire i figli nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC (Tecnologie Informazione Comunicazione) indicate dai docenti, in particolare controllare l'utilizzo corretto 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.

• Fissare delle regole generali per l'utilizzo del computer, degli altri strumenti digitali quali smartphone, tablet o dispositivi per la registrazione audio/video e tenere sotto controllo l'uso che i figli fanno di internet e delle risorse in esso presenti.

- Condivisione e comunicazione della Policy all'intera comunità scolastica.

Il documento verrà condiviso e comunicato agli alunni, a tutto il personale della scuola e ai genitori. Le regole relative all'accesso ad Internet vengono approvate dal Collegio dei Docenti e pubblicate sul sito istituzionale.

Gli alunni saranno istruiti riguardo l'uso responsabile e sicuro di internet e saranno informati che per l'utilizzo della Rete a scuola e di ogni altro dispositivo digitale gli insegnanti ne autorizzeranno e controlleranno l'uso. A tale scopo il Regolamento per la sicurezza on-line sarà letto e illustrato dai docenti e pubblicato in tutte le aule e spazi con accesso a internet.
Inoltre per favorire una maggiore consapevolezza sull'uso sicuro e responsabile di internet tra gli alunni saranno realizzate delle lezioni informative/formative da parte dei docenti del Web Staff del progetto "Generazioni Connesse".

Il personale della scuola sarà informato/formato sulla politica della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet tramite il presente documento, materiale informativo, incontri e riunioni istituzionali (consigli di interclasse/intersezione, collegio dei docenti). Il personale docente sarà informato del fatto che l'utilizzo di internet attraverso le infrastrutture scolastiche (di tipo hardware e software) sarà monitorato e si potrà risalire al singolo utente registrato.

I genitori degli alunni saranno informati/formati sulla politica della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet tramite il presente documento, materiale informativo e incontri di vario genere (assemblee, seminari, riunioni scuola-famiglia). Lo scopo è quello di favorire una maggiore collaborazione nel perseguimento della sicurezza nell'utilizzo sicuro delle tecnologie digitali e di internet anche a casa.
In particolare si informeranno i genitori sui sistemi di filtraggio per la navigazione su internet e sulle attività educative per il tempo libero.

- Gestione delle infrazioni alla Policy.

1) Le potenziali infrazioni in cui è possibile che gli **alunni** incorrano a scuola nell'utilizzo delle tecnologie digitali e di internet per fini didattici sono prevedibilmente le seguenti:

• Condivisione di immagini intime o "contrarie al decoro".

• Comunicazione incauta e senza permesso con sconosciuti.

• Collegamento a siti web non indicati dai docenti.

• Diffusione impropria (con o senza il consenso della persona interessata) di dati in formato audio, video o immagine che riproducono registrazioni vocali o filmati o fotografie digitali riconducibili a persone, alunni e docenti, o altri soggetti, che operano o si trovino all'interno della scuola.

In relazione all'età e alla gravità delle infrazioni sono previsti i seguenti provvedimenti disciplinari:

• Richiamo verbale.

• Richiamo scritto sul registro di classe o con annotazione sul diario.

• Convocazione dei genitori da parte degli insegnanti.

• Convocazione dei genitori da parte del Dirigente scolastico.

2) Le potenziali infrazioni in cui è possibile che il **personale scolastico** e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono:

• Utilizzo delle tecnologie e dei servizi della scuola non connesso alle attività di insegnamento o al profilo professionale, come ed a titolo esemplificativo e non esaustivo l'installazione di software o lo scaricamento e il salvataggio di materiali non idonei o non consentiti dalla legge.

• Utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale.

• Trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi.

• Diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi.

• Scarsa vigilanza degli alunni che può favorire un utilizzo non autorizzato delle TAC e possibili incidenti fisici per le persone o comportamenti malevoli o dannosi.

• Insufficienti interventi nelle situazioni critiche e mancata segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TAC 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. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e con l'Animatore digitale e a fornire ogni informazione utile per la risoluzione di eventuali situazioni problematiche connesse all'uso delle TAC e Internet.

3) Alcune condotte dei **genitori** possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola.
Per esempio alcune famiglie sottovalutano i potenziali rischi a cui espongono i figli se permettono loro di:

• Rimanere a casa da soli ad usare il computer.
• Avere un computer nella propria stanza o in un posto non visibile.
• Navigare sul web, utilizzare il cellulare o lo smartphone senza nessun controllo.
• Utilizzare il pc o cellulare o smartphone in comune con gli adulti che possono conservare in memoria materiali non idonei.

I genitori degli alunni 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 Policy e suo aggiornamento.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dei docenti del Web Staff costituitosi in occasione del progetto "Generazioni Connesse", tramite questionari e conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

- Integrazione della Policy con Regolamenti esistenti.

La policy costituisce parte integrante del Regolamento di Istituto.

2. Formazione e Curricolo

- Curricolo sulle competenze digitali per gli studenti

In linea con il sistema scolastico europeo, la scuola italiana assume come orizzonte di riferimento verso cui tendere il quadro delle competenze-chiave per l'apprendimento permanente definite dal Parlamento europeo e dal Consiglio dell'Unione europea nel 2006.

Tra le otto competenze necessarie per il life long learning, troviamo la cosiddetta "competenza digitale" che viene così definita: "La competenza digitale 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 TAC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet." È annoverata tra le competenze trasversali necessarie alla cittadinanza poiché permette di accedere ai saperi.

Parlando di competenza digitale non si fa riferimento soltanto alle semplici abilità informatiche di base alle quali tutti siamo abituati attraverso l'uso quotidiano del computer, ma anche alla capacità di saper ricercare e trattare criticamente e responsabilmente le informazioni.

Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali 2012: infatti la competenza digitale non rappresenta una disciplina autonoma, ma appare come un ambito che gli alunni possono sviluppare trasversalmente attraverso le altre attività didattiche. Competenza digitale significa infine 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 ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

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

L'esplosione di Internet e la globalizzazione della rete, la diffusione dei Social Network e dei Social Software del web 3.0, stanno sempre più orientando le giovani generazioni verso nuove forme di apprendimento informale, autodiretto, partecipativo.

In questo contesto, le istituzioni educative pur non essendo più il luogo esclusivo di produzione della conoscenza e nemmeno quello di acquisizione dei contenuti, mantengono però una funzione che non può essere sostituita oggi da nessuna tecnologia, quella di facilitazione dei processi di

apprendimento, di sostegno allo sviluppo delle facoltà cognitive, di guida all'acquisizione di competenze che consentono a ogni allievo di liberare le sue potenzialità e divenire parte attiva nella società.

Esattamente in questa direzione si muove il Piano Nazionale per la Scuola Digitale (PNSD) previsto nella legge 107/2015.

Il documento ha funzione di indirizzo; punta a introdurre le nuove tecnologie nelle scuole, a diffondere l'idea di apprendimento permanente (lifelong learning) ed estendere il concetto di scuola dal luogo fisico a spazi di apprendimento virtuali.

Con il PNSD le tecnologie entrano in classe e supportano la didattica, permettono a studenti e docenti di interagire con modalità didattiche costruttive e cooperative attraverso apps da sfruttare come ambienti o strumenti di apprendimento, superando l'impostazione frontale della lezione e favorendo una didattica meno trasmissiva e più operativa.

Questo presuppone nuovi compiti per l'insegnante che dovrà essere in grado di creare negli studenti familiarità e pratica con le nuove tecnologie, intese come strumenti che servono a produrre una nuova forma di sapere e una nuova organizzazione delle conoscenze.

Non si tratta tanto di insegnare l'uso tecnico di specifici programmi quanto di far acquisire agli alunni una *forma mentis* tecnologica, orientata alla comprensione di funzioni generali e alla capacità di saper selezionare e inquadrare le tecnologie nei particolari contesti d'uso.

In quest'ottica si accompagneranno gli alunni a comprendere: come selezionare in modo accurato materiale e informazioni reperite da varie risorse; come sviluppare e presentare le proprie idee, monitorando e migliorando la qualità del proprio lavoro; come scambiare e condividere informazioni; come rivedere, modificare e valutare il proprio lavoro riflettendo criticamente sulla sua qualità anche mentre lo si sta realizzando.

È importante, allora, che i docenti comprendano il funzionamento generale delle più diffuse strumentazioni informatiche, per poterne cogliere il potenziale didattico e valutarne poi l'utilizzo in maniera consapevole e critica. È ancora troppo diffusa la concezione che le TAC siano principalmente un ottimo medium, inteso unicamente come veicolo passivo per la trasmissione di conoscenze (si pensi all'utilizzo riduttivo della LIM come semplice schermo per condividere filmati e risorse da internet).

Le TAC favoriscono attività di co-costruzione degli oggetti di apprendimento (ad esempio mappe concettuali e mentali, learning objects,…), di documentazione e accesso ai contenuti (ad esempio piattaforme come Moodle, blog,…) per la loro successiva rielaborazione in un'ottica di personalizzazione e individualizzazione ovvero di personale costruzione di nuovi significati e materiali.

Le nuove tecnologie richiedono agli insegnanti nuovi compiti, approcci didattici e come previsto nel PNSD devono prevedere nuovi percorsi formativi.

L'integrazione reale delle TAC in classe dipende anche dalla capacità degli insegnanti di progettare l'ambiente di apprendimento in modo non tradizionale, di unire le nuove tecnologie alle nuove forme di didattica, di sviluppare classi socialmente attive, incoraggiando l'interazione cooperativa, l'apprendimento collaborativo, il lavoro di gruppo.

Nel corso di quest'anno scolastico il nostro Istituto ha previsto le seguenti attività di formazione per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'uso delle TAC:

- Corso per tutto il personale docente sull'uso delle Lim.
- Corso introduttivo alla gestione delle piattaforme per l'applicazione della metodologia della classe capovolta (Flipped classroom) in tutte le classi prime della scuola secondaria di primo grado.
- Diffusione di materiale informativo e incontri in presenza tra gruppi di docenti sulle seguenti tematiche: gestione delle piattaforme e delle applicazioni online utili alla didattica; nuove tecnologie per l'inclusività, video e tutorial.
- Partecipazione alla settimana digitale con il Progetto "Code week" con la presenza di più del 50% di studenti, con la sperimentazione della metodologia del coding al fine di promuovere lo sviluppo negli alunni del "pensiero computazionale".

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

Oggi la scuola se da una parte si trova di fronte alla necessità di incorporare le nuove tecnologie nei metodi di insegnamento, e di diffonderne il corretto uso, dall'altra deve tener conto dei rischi connessi.

Bambini e ragazzi, navigando in Rete, possono trovarsi di fronte a materiali e contenuti inadeguati per la loro età (ad esempio, contenuti violenti, con espliciti riferimenti sessuali o che incitano al razzismo) o interagire con soggetti malintenzionati che possono ingannarli ed invitarli a comportamenti o azioni che possono costituire un pericolo.

Oltre ai contenuti di natura sessuale, Internet può veicolarne altri che, pur essendo altrettanto pericolosi, spesso non sono oggetto della medesima attenzione. Ne sono un esempio, l'esaltazione della violenza e della crudeltà, l'istigazione all'odio e al razzismo, la pubblicità di tabacco e alcool o di giochi d'azzardo magari descritti come privi di rischio, così come la valorizzazione dell'estrema

magrezza ed il ricorso a qualsiasi mezzo per raggiungerla, il mito dell'arricchimento facile ed il ricorso a comportamenti illegali per ottenere un guadagno immediato. Tali messaggi possono essere particolarmente forti e convincenti soprattutto per chi, come un giovane fruitore, non è ancora in grado di comprenderli appieno.

Le stesse modalità di utilizzo di Internet possono essere inadeguate per la crescita di bambini e adolescenti. Navigando tra un link e l'altro, infatti, è possibile perdere la cognizione del tempo, sottovalutando l'importanza di attività fondamentali per una sana crescita psicofisica quali lo studio, le amicizie e lo sport. Alcune ricerche condotte negli ultimi anni hanno evidenziato i rischi psicologici che un uso eccessivo o distorto della Rete comporta; in situazioni particolari, si possono sviluppare delle vere e proprie dipendenze che necessitano l'intervento da parte di professionisti. Non bisogna dimenticare anche altre situazioni che, pur non incidendo direttamente sullo sviluppo dei giovani cybernauti, risultano comunque essere indesiderate: tra queste, il pericolo di installare virus informatici che danneggiano il pc o che trasmettono nel web documenti riservati; il rischio di essere vittime di truffe, di commettere azioni illegali (ad esempio, violando le leggi sul diritto d'autore) ed essere oggetto di veri e propri bombardamenti pubblicitari.

Consapevoli delle potenzialità, così come dei rischi e pericoli connessi all'utilizzo delle tecnologie, la scuola con la comunità dei suoi docenti è chiamata a guidare tutti i soggetti in situazione di apprendimento, in particolare gli studenti, e a sviluppare le competenze per costruire una cittadinanza digitale attiva e responsabile.

Nel corso di quest'anno scolastico il nostro Istituto, in occasione del progetto "Generazioni Connesse", ha realizzato la diffusione e condivisione di materiale informativo sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, dal sito "Generazioni connesse", ecc.

- Sensibilizzazione delle famiglie

L'Istituto ha previsto diverse iniziative per sensibilizzare le famiglie all'uso consapevole delle TAC e della Rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti 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 coetanei

e non con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel presente documento, *Policy e-safety*, per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola

- Accesso a internet: filtri, antivirus e sulla navigazione

• La scuola è dotata di un sistema di protezione (firewall evoluto). L'accesso ad internet tramite il "WebON" (pagina personalizzata della scuola) è richiesta in modo esplicito e volontario dall' utente ed è regolamentato dai suoi privilegi di sistema. Gli utenti sono raggruppati in modo che l'Amministratore di sistema possa gestire modalità di accesso ad Internet differenziate per gruppo (ad es. per uffici, docenti, alunni).

• La scuola tramite dei sistemi di controllo traccia gli accessi e le attività degli utenti su internet, secondo le normative vigenti e produce dei file di log ad archiviazione automatica periodica, in modo che sia possibile al Dirigente Scolastico rispondere facilmente e pienamente ad eventuali richieste delle Autorità competenti.

• È impedito l'accesso ai siti web e domini internet non idonei all'ambito scolastico (funzionalità di "parental control") o, in modo simmetrico, ciò è consentito solo per i siti e i domini di interesse. I controlli sono esercitati non solo sulle attività di navigazione web, ma anche sulle app degli smartphone e/o per protocollo di comunicazione.

È disponibile un servizio online di gestione delle liste d'accesso (in particolare di quelle non idonee – "blacklist").

- Gestione accessi (password, backup, ecc.)

L'accesso agli strumenti informatici è consentito solo previa autenticazione personale effettuata mediante sistema di identificazione (attribuzione individuale di nome utente e password).

Ciascun utente è personalmente responsabile per l'uso del proprio account ed è tenuto a tutelarlo da accessi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.

La password è personale, riservata e non può essere ceduta o comunicata ad alcuno. È pertanto

vietato l'uso della password di altri utenti; qualora se ne venisse a conoscenza è obbligatorio segnalare il fatto all'utente interessato, al docente responsabile e all'Amministratore di sistema.
È obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta.
Per esigenze operative o di sicurezza e integrità del sistema e dei dati, l'Amministratore di sistema (Animatore digitale) ha facoltà di modificare la password degli utenti o di disabilitarle.

- E-mail.

L'Istituto ha un account di posta elettronica istituzionale utilizzato esclusivamente dagli uffici amministrativi. La posta elettronica è protetta da sistemi antivirus, e quella certificata anche da sistemi antispam.

- Blog e sito web della scuola

La scuola attualmente ha un sito web, un canale Youtube ed una Web Tv in allestimento. Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione dell'Animatore digitale, che ne valuta con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

- Social network.

L'istituzione scolastica ha una pagina su Facebook in cui vengono pubblicati eventi, attività realizzati dalla scuola. Solo l'Amministratore della pagina Facebook (Animatore digitale) può postare e commentare le varie notizie.
La scuola, inoltre, utilizza la piattaforma Edmodo per la gestione delle classi come gruppi virtuali. Edmodo offre la possibilità di gestire gruppi di utenti per collegarsi e collaborare, produrre e condividere contenuti, accedere a compiti, effettuare test e quiz, ottenere valutazioni. È un ambiente sicuro e controllato, in quanto si accede con password personale, ed è semplice nell'uso, in quanto non richiede alcuna installazione di hardware o software sui dispositivi degli utenti. Le password sono fornite agli alunni previa autorizzazione dei genitori che si assumono la responsabilità dell'uso della piattaforma. Ai genitori viene consegnato un codice per controllare le attività on line dei figli.

- Protezione dei dati personali.

La scuola ha l'obbligo di far conoscere agli studenti e alle loro famiglie come usa i loro dati personali. Deve cioè rendere noto, attraverso un'adeguata informativa, quali dati raccoglie e come li uti-

lizza.

La scuola è tenuta a chiedere il consenso per il trattamento dei dati personali degli studenti.

Gli unici trattamenti permessi sono quelli necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore.

Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

Alcune categorie di dati personali degli studenti e delle famiglie – come quelli sensibili e giudiziari – devono essere trattate con estrema cautela, verificando prima non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "rilevanti finalità pubbliche" che si intendono perseguire.

4. Strumentazione personale

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

Durante lo svolgimento delle attività didattiche è vietato l'uso dei cellulari e di altri dispositivi elettronici. L'uso del cellulare è consentito solo in caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione e con controllo dell'identità dell'interlocutore verificata dal docente.

L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante l'attività didattica deve essere autorizzato dal docente. A tal proposito sarà ovviamente consentito l'uso di dispositivi mobili personali durante le attività didattiche che ne prevedano l'utilizzo, secondo la metodologia BYOD (Bring your own device)

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

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

- Per il personale della scuola: gestione degli strumenti personali– cellulari, tablet ecc.

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

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

Alcuni comportamenti scorretti e potenzialmente dannosi per sé e per gli altri sono spesso conseguenza di un uso ingenuo e superficiale di internet. Queste situazioni appaiono già pericolose in quanto molto spesso derivano da procedure consuete nell'uso di strumenti in rete che possono indurre chiunque a sottovalutare i rischi connessi ad un uso disinvolto di questi mezzi. I comportamenti quasi aggressivi finiscono per arrivare all'attenzione degli adulti, sono controllati e contenuti dai docenti con normali interventi educativi, in modo da evitare che possano degenerare diventando pericolosi per sé e per gli altri. I comportamenti quasi aggressivi e quelli già riferibili al bullismo possono esprimersi in varie forme ma è sempre di fondamentale importanza che ciascuno degli attori (Scuola e Famiglia) sappia con certezza come comportarsi per una buona riuscita dell'intervento educativo.

Telefoni cellulari

Il telefono cellulare, nell'ormai comune versione dello smartphone, permette di parlare e scrivere messaggi ma anche di scaricare e spedire foto, audio e video, accedere ad internet, leggere la posta elettronica, ascoltare musica e giocare con i videogiochi. Dunque il telefono cellulare permette a chiunque di contattare ed essere contattato e questo fa sì che un bullo o un malintenzionato in genere, possano fare di questo strumento un uso non corretto: fare telefonate moleste, spedire fastidiosi messaggi, condividere immagini umilianti, riprendere con la videocamera del telefono atti di bullismo o di aggressione o di scherno per poi diffonderli.

I contenuti possono essere postati on line, spediti da telefono cellulare a telefono cellulare, condivisi usando una connessione senza fili e quindi bypassando l'operatore telefonico (es. bluetooth o infrarossi).

Messaggi istantanei (IM)

I programmi di messaggeria istantanea (IM) permettono di vedere quali contatti sono in linea e di chattare tramite testo o audio e video mentre si usa il computer. Contrariamente ad altre chatrooms, che sono tipicamente pubbliche e aperte all'iscrizione di chiunque, IM è più privata e di solito la conversazione avviene tra due persone. Ad esempio, fra i tanti software di IM, Windows Live Messenger (chiamato MSN Messenger) è il più popolare e i ragazzi solitamente la utilizzano come estensione della loro vita sociale, per comunicare con gli amici lontano dalla scuola. È molto veloce, permette di stare in contatto e può essere considerato un moderno strumento per socializzare. Purtroppo anche in questo caso un uso non corretto provoca disagi e problemi piuttosto seri.

E-mail

La posta elettronica è oggi una parte essenziale della vita professionale e relazionale delle persone. Permette di trasmettere messaggi in tempo reale da un PC ad un altro, utilizzando la rete internet, è un utile strumento di comunicazione. Anche la posta elettronica potrebbe essere soggetta ad uso improprio e ad eventuali manomissioni. Messaggi molesti e minacciosi possono essere spediti senza conoscere necessariamente il bersaglio.

Bambini e ragazzi dovrebbero essere messi al corrente del rischio insito nel pubblicare informazioni private o nel fare amicizia con persone, potenzialmente pericolose, le quali, pur di creare un contatto, possono mentire sulla propria identità.

Chat

La chat è una conversazione (testo o voce e video) in tempo reale. È un servizio aperto a tutti, previa registrazione attraverso un nickname, dietro il quale spesso le persone assumono differenti identità, sentendosi così libere da vincoli sociali quali l'età, l'identità etnica o l'aspetto fisico e sociale. Per i ragazzi molto timidi può risultare un facile modo per incontrare e conoscere nuove persone. Ma proprio per la mancanza di conoscenza diretta dell'interlocutore le chatrooms possono essere frequentate da chiunque: bambini, ragazzi, adulti. Tuttavia, nessuno resta del tutto anonimo.

Ogni nickname è, infatti, associato ad un numero IP per tutto il tempo che l'utente resta nella chat e questo permette, se necessario, all'Amministratore di sistema di rintracciare la reale identità.

Siti di social networking

I siti social networking sono stati pensati per aiutare le persone a trovare nuovi amici e comunicare con loro. In questi siti (ad esempio, e solo per citare i più noti, Facebook, Twitter, MySpace, Badoo,) l'utente può creare una pagina col proprio profilo, inserendo i suoi interessi e ulteriori dettagli, per essere contattato da altri potenziali amici da aggiungere alla sua lista. I più giovani, ma non solo, utilizzano lo spazio on line per socializzare con altre persone e molti ne fanno un punto di riferimento per le loro attività, spendendo molto tempo nel guardare i profili degli altri e nel costruire le nuove pagine in cui spesso sono inseriti dettagli ed informazioni personali proprie e di amici. Anche attraverso i social network possono essere spediti messaggi molesti, diffamatori e minacciosi, utilizzando le informazioni inserite nei profili; per questo è importante far capire ai bambini e ragazzi quanto potrebbe essere rischioso pubblicare informazioni private o fare amicizia con persone, potenzialmente pericolose.

Per concludere diverse sono le tipologie di uso improprio classificabili come atti di cyberbullismo

- **Molestie - Harrassment**: messaggi e pubblicazioni offensive o volgari, ripetuti nel tempo; spyware – controllo delle attività on line della vittima; telefonate mute.
- **Cyberstalking:** può nascere quando la molestia è particolarmente insistente e diretta verso coetanei e non con cui si ha un rapporto conflittuale o con cui si è interrotta una relazione affettiva.
- **Denigrazione - Denigration:** azione singola volta a denigrare l'altro (ad esempio e a titolo puramente esemplificativo, una foto deformata, immagini pornografiche, materiale audio o video di scherno) che può produrre effetti imprevedibili e a cascata.
- **Fingersi un altro – Impersonation:** il bullo, riuscito ad accedere alla password della vittima, invia messaggi ad altre persone o pubblica dati, "spacciandosi" per quella persona, al fine di cambiare o distruggere l'immagine della stessa.
- **Manipolazione delle informazioni – Outing:** "il bullo" conosce segreti e possiede immagini della "vittima" (prima amica) che diffonde a sua insaputa o contro la sua volontà. Può costringere la "vittima" a pubblicare informazioni e/o immagini di altre persone.
- **Escludere ("bannare") - Exclution:** cancellare/estromettere da una chat, o da un gruppo on line di gioco, oppure da una lista di amici, una persona.

- **Filmare – Cyberbrashing:** videoriprendere un atto di bullismo e pubblicarlo su internet, chiedendo pareri e di condividerlo.
- **Flaming** – dal termine "*fiamma*": invio online di messaggi violenti e volgari.
- **Rivelazione**: pubblicazione di informazioni o immagini imbarazzanti su qualcuno.
- **Cyberpersecuzione**: molestie e minacce ripetute per incutere timore o paura

Rilevazione e Gestione dei casi

Tutte le azioni e le attività messe in campo mireranno innanzitutto a prevenire tramite la sensibilizzazione al linguaggio emotivo, che gli studi hanno trovato carente sia nei bulli che nelle vittime, al miglioramento delle competenze nelle "social skills".

Le procedure interne per la rilevazione e la gestione dei casi, nonché la segnalazione alla Dirigenza Scolastica ed eventualmente alle autorità competenti, avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse". Ciascuna componente, scolastica e non, opererà secondo il proprio ruolo.

Docente:

- Durante la lezioni osservare attentamente le varie dinamiche attentive e possibili varianti comportamentali e di umore dei discenti.
- Durante i momenti ricreativi osservare attentamente le dinamiche relazionali tra il gruppo dei pari e con i docenti.
- Conservare ordinandoli in una database e aggiornato dal Web Staff referente i comportamenti cyberbullistici (video, messaggi offensivi, di cui si viene a conoscenza).
- Segnalare (alle Forze dell'Ordine) i comportamenti cyberbullistici (video, messaggi offensivi, di cui si viene a conoscenza).
- Confiscare il telefono che contiene il materiale offensivo e chiedere agli studenti (attraverso ascolti individuali) di indicare a chi e dove tale materiale sia stato spedito.
- Contattare la polizia se si ritiene che il materiale offensivo sia illegale (ad esempio e solo a titolo esemplificativo, video pornografici).
- Cancellare il materiale offensivo dal dispositivo, dopo avere provveduto a farne una copia.
- Riservare una quota del monte ore mensile per confronti all'interno della classe (circle time) conversazioni guidate o libere.

- Costituzione di un "Web Staff" d'Istituto, che si occupi di supportare i docenti nella gestione dei casi più problematici. Il "Web staff" sarà composto da: Dirigente Scolastico, cinque docenti (due della scuola Primaria e tre della scuola Secondaria di primo grado) e dall'Animatore digitale. I componenti dello staff seguiranno appositi corsi di formazione tenuti da specialisti sociosanitari, operatori di pubblica sicurezza e tecnici informatici.

-Come segnalare: quali strumenti e a chi

Individuata l'eventuale problematica, attivare i vari protocolli di analisi ed intervento:
CODICE 1. PRIORITA' BASSA
CODICE 2. PRIORITA' MEDIA
CODICE 3. PRIORITA' ALTA

CODICE 1
Il docente dopo attenta valutazione del caso, e dopo giusta consultazione con il D.S. e il coordinatore della classe, gestirà la dinamica in autonomia, coinvolgendo, se opportuno la/le famiglia/e successivamente relazionerà al D.S. e al consiglio di classe sulla evoluzione o risoluzione del caso.

CODICE 2
Il docente dopo aver verificato la gravità del caso, dopo aver consultato il D.S., richiederà la consulenza dello staff, e in sinergia si concorderanno le linee più opportune da seguire.
Naturalmente saranno informate le famiglie sulle dinamiche del caso.
L'intera gestione del caso dovrà essere debitamente verbalizzata e protocollata in un registro dedicato e riservato a cura del dirigente scolastico.

CODICE 3
Caso di competenza esterna alla gestione scolastica.
Il docente dopo la rilevazione del caso, verbalizzerà l'accaduto, su apposito modello, e in sinergia con D.S. e Web staff trasmetterà agli organi di competenza (Sert, Polizia di Stato, Polizia locale, Procura della Repubblica)
La panoramica d'intervento è destinata a tutti i docenti in servizio presso l'istituzione scolastica; ed è naturalmente allargata, per le proprie responsabilità, al personale A.T.A.. (culpa in vigilando e culpa in educando).

Il ruolo della famiglia:

- Osservare il comportamento dei ragazzi dopo la navigazione in internet o l'uso del telefonino (stati ansiosi, depressivi, etc).
- Aiutare i ragazzi a riflettere sul fatto che anche se non vedono la reazione delle persone a cui inviano messaggi o video, esse possono soffrire.
- Educare i ragazzi ad utilizzare il dialogo quando nascono conflitti.
- Controllare e monitorare le amicizie e i siti frequentati dai propri figli, condividendo con loro le motivazioni di tale controllo.

Segnali dei ragazzi ai quali i prestare attenzione

- Si rifiutano di parlare di ciò che fanno online.
- Utilizzano Internet fino a tarda notte.
- Fanno un uso eccessivo di Internet.
- Hanno un calo dei voti scolastici.
- Sono turbati dopo aver utilizzato Internet.

Cosa i ragazzi devono sapere:

- Non dare informazioni personali, come nome, indirizzo, numero di telefono, età, nome e località della scuola o nome degli amici, a chi non si conosce personalmente o a chi si conosce soltanto sul web.
- Non condividere le proprie password, neanche con gli amici.
- Non accettare incontri di persona con qualcuno conosciuto online.
- Non rispondere a messaggi che facciano sentire confusi o a disagio. Meglio ignorare il mittente, terminare la comunicazione e riferire quanto accaduto a un adulto.
- Non usare un linguaggio offensivo o mandare messaggi volgari online.
- Chiedere il permesso alla persona interessata, prima di pubblicare un'immagine o video su un blog, un social network o qualsiasi altro servizio online.
- Se si riceve materiale offensivo non pubblicarlo, quanto piuttosto conservarlo e informare un adulto.
- Cambiare le proprie password periodicamente e non utilizzare un'unica password per tutti i propri servizi online.