Sede esami
Centre number: 29114

ISTITUTO COMPRENSIVO "SAN G. BOSCO"
Via Nuova 74016 MASSAFRA (TA) tel. 099/8801180
e-mail taic851009@istruzione.it
e-mail PEC taic851009@pec.istruzione.it
Codice Fiscale: 90214650732
www.icsgboscomassafra.gov.it

Nr. 0012037

E-Safety Policy

IC "SAN G. BOSCO" MASSAFRA -TA-

a.s. 2017/2018

INDICE RAGIONATO

1. INTRODUZIONE

1.1. Scopo della policy.

Scopo del presente documento è quello di informare le parti interessate e predisporre ad un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa cogente. In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni 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 tecnologie digitali. Gli utenti, siano essi maggiorenni o minorenni, anche se "nativi digitali", non sempre sono pienamente consapevoli dei rischi a cui si espongono quando navigano in rete.
In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.
L'e- *policy* si applica a tutti i membri della comunità scolastica che hanno accesso al sistema informatico della scuola.

1.2. Ruoli e responsabilità (che cosa ci si aspetta da tutti gli attori della comunità scolastica).

Dirigente Scolastico

È responsabile della presentazione del documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti; valuta l'efficacia della politica e ne monitora l'attuazione, anche in collaborazione con il team digitale. A tale scopo è fondamentale ricevere tempestive informazioni sulle violazioni al presente regolamento dal corpo docente o dal personale ATA che ne vengano a conoscenza.

Direttore dei servizi generali e amministrativi

Assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; garantisce il funzionamento dei diversi canali di comunicazione della scuola all'interno e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni sia del Dirigente, sia dei docenti.

Team digitale

Cura la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicura la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola.
Si relaziona con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune; riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

Personale docente - con particolare riferimento ai responsabili di plesso, ai coordinatori dei consigli di classe, ai presidenti di interclasse –

I docenti sono tenuti a:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o al team digitale per le opportune indagini / azioni / sanzioni;

- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- integrare i problemi di sicurezza informatica in tutti gli aspetti del curricolo di studi e in altre attività extracurricolari;
- far comprendere e far mettere in pratica a tutti i fruitori della rete le regole di comportamento relative alla sicurezza informatica;
- favorire negli studenti una buona cognizione in merito alla normativa sul diritto d'autore per evitare il plagio e/o l'illecita diffusione di dati personali;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, durante le lezioni e/o altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- guidare la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati onde evitare di imbattersi in materiali inadatti.

Personale ATA

- Conosce le norme della policy
- Contribuisce alla sorveglianza

Alunni/studenti

Gli alunni/studenti sono responsabili per l'utilizzo dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti dalla seguente policy. In particolare sono tenuti a:

- non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente:
- gestire con cognizione le fasi di ricerca sul web per evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo.
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato. La scuola coglierà ogni occasione per sensibilizzare i genitori circa questi problemi attraverso: incontri con la Polizia postale ed altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-safety e a seguire le linee guida sull'uso appropriato di:

- immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule
- accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- dispositivi personali dei loro figli nella scuola (dove ciò è consentito).

1.3. Condivisione e comunicazione della policy all'intera comunità scolastica.

Per evitare che l'adozione di questa policy rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire **dalla pubblicazione sul sito della scuola**, si possono ipotizzare per esempio:

Per il corpo docente:

- discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della policy;
- un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;
- elaborazione di protocolli condivisi di intervento.

Per gli alunni/studenti:

- la discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime;
- l'inserimento di un estratto di questo documento nel diario scolastico e in particolare dei comportamenti da attuare in caso di bisogno.

Per i genitori:

Saranno organizzati incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare. In Particolare:

- l'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nell'area PNSD del sito web della scuola;
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari e individuali;

1.4. Gestione delle infrazioni della policy.

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA.
Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale).
L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

- Minaccia, in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 codice penale);
- Pedopornografia (art. 600ter);
- Corruzione di minorenne (art. 609quinquies).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.
Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

1.5. Integrazione della policy con Regolamenti esistenti.

La presente policy è allegata in appendice al PTOF.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli alunni/studenti.

Lo sviluppo delle competenze digitali e in generale della consapevolezza digitale è fondamentale all'interno dell'odierna struttura socio-economica. La scuola ha il dovere di: * sviluppare competenze digitali e rendere fruibili le apparecchiature informatiche come parte integrante della esperienza di apprendimento. L'uso delle TIC va inserito pertanto nel curricolo sia a livello disciplinare sia a livello interdisciplinare.

In particolare il curricolo dovrà essere strutturato per prevedere di:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia in ambienti condivisi;
- insegnare la valutazione dei contenuti Internet;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- rendere alunne e alunni criticamente consapevoli dei materiali che si leggono sul web allo scopo di vagliare le informazioni prima di accettarne la fondatezza, la coerenza, le origini;
- mostrare la segnalazione di contenuti Internet sgradevoli o illegali.

Inserita nelle otto Competenze chiave di cittadinanza attiva indicate dal Consiglio di Lisbona nel marzo 2000, la Competenza *digitale* viene così definita all'interno della Raccomandazione del Parlamento europeo e del Consiglio del 18 dicembre 2006, relativa a competenze chiave per l'apprendimento permanente (2006/962/CE):

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione 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.

La Competenza digitale è *trasversale* alle discipline previste dalle Indicazioni Nazionali 2012; in tutte le discipline si ritrovano *abilità* e *conoscenze* che fanno capo alla competenza digitale e tutte concorrono a costruirla.

Competenza digitale significa padroneggiare 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.

APPRENDIMENTI DIGITALI ALLA FINE DELLA SCUOLA DEL PRIMO CICLO		
CONOSCENZE	**ABILITÀ**	**COMPETENZE**
Il sistema operativo e i più comuni software applicativi, con particolare riferimento *all'office automation* e ai prodotti multimediali anche *Open source*. Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi. Caratteristiche e potenzialità tecnologiche degli strumenti d'uso più comuni. Fonti di pericolo e procedure di sicurezza. Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche.	Utilizzare materiali digitali per l'apprendimento. Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni: Procedure per la produzione di testi, ipertesti, presentazioni. Procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati, fare ricerche e comunicare (motori di ricerca, sistemi di comunicazione mobile, email, chat, social network, protezione degli account, download, diritto d'autore, ecc.)	Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio. Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.

2.2 Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF e nell'ambito delle azioni del PNSD, si prevede che una parte della formazione in servizio, ai sensi della L. 107/2015, sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta da docenti dell'Istituto che fanno parte del team digitale, per cui il MIUR prevede opportuni percorsi la cui ricaduta viene annualmente tarata secondo le esigenze formulate dal Collegio Docenti, ed è improntata alla condivisione di esperienze significative e di buone pratiche.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola può aderire a progetti appositi di formazione presentati da enti e associazioni.

2.3 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 della Rete, 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 i ragazzi.

2.4 Sensibilizzazione delle famiglie.

La dirigenza promuoverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC, della Rete e delle tipiche 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 i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Nello specifico, per l'a.s. 2017/2018 è previsto un laboratorio PON destinato ai genitori: "Educazione ai Soci@l"
Sul sito scolastico, nell'area PNSD, saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato *pdf* e video che possono fornire spunti di approfondimento e confronto.
La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento di **e-Safety Policy** 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.

Attualmente il nostro Istituto è connesso ad internet tramite collegamento wireless. Gli alunni possono usufruire della connessione negli ambienti dedicati: laboratori e isole digitali, con il controllo del docente.
È in fase di realizzazione il potenziamento della rete.

3.1 Accesso ad internet: filtri, antivirus e sulla navigazione.

Nel nostro IC tanto la segreteria, quanto i laboratori e le isole digitali sono provvisti di dispositivi di sicurezza, e di antivirus. Il DSGA e il team digitale monitorano periodicamente il funzionamento provvedendo, in tempi brevi, a contattare la ditta appaltata per la manutenzione in caso di guasto o malfunzionamento.

3.2 Gestione degli accessi

Attualmente gli alunni accedono tramite password personale (controllata e ridefinibile dal docente) solo alla piattaforma Edmodo che viene utilizzata in alcune classi per la condivisione di materiale di supporto allo studio.. Ciascun utente connesso alla rete dovrà, tuttavia, rispettare il presente regolamento e la legislazione vigente, la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la netiquette.
I genitori saranno invitati a firmare e restituire un modulo di consenso. Gli alunni dovrànno impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

3.3 E-mail.

Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola o all'interno della piattaforma di apprendimento, per consentire l'attivazione di protocolli di controllo.
E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

3.4 Sito web della scuola.

La scuola è dotata di sito internet: www.icsgbosomassafra.gov.it
Il sito si configura come un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali e avvisi di carattere generale.
L'inserimento dei contenuti è possibile agli addetti del personale di Segreteria, per quanto riguarda i dati di tipo economico-amministrativo, mentre l'animatore digitale gestisce le pagine descrittive dell'Istituto e delle attività che vi si svolgono.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato, anche e soprattutto ai fini del rispetto del Codice dell'Amministrazione Digitale (CAD).

3.5 Social network.

Nella pratica didattica si cerca di educare gli alunni all' uso sicuro dei siti di social networking. Per questo, grosso riferimento è la piattaforma di "generazioni connesse".
Alunne/alunni, genitori e personale docente/ATA saranno informati sull'uso sicuro degli spazi di social network e sulle conseguenze legali di ogni uso improprio Agli alunni è fatto divieto di pubblicazione, senza permesso, di foto personali proprie o altrui su qualsiasi spazio di social network previsto nella piattaforma di apprendimento scolastico.
Alunne e alunni saranno invitati a usare nickname e avatar non riconoscibili quando utilizzano siti di social networking.

3.6 Protezione dei dati personali.

Si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy).

4. STRUMENTAZIONE PERSONALE

4.1 Per la componente studentesca.

I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni se non all'interno di attività didattiche espressamente programmate dal corpo docente.
Per gli alunni con disturbi specifici di apprendimento, si concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia degli stessi.
Nel caso in cui sia necessario comunicare con la famiglia durante l'orario scolastico, alunne e alunni potranno usare la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie possono chiamare a scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

4.2 Per il personale docente/ATA.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, …); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali.
Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate.
La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).
Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.
Durante l'attività didattica è opportuno che ogni insegnante: - dia chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli studenti la netiquette e indicandone le regole; - si assuma la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico; - non salvi sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili e proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

4.3 Utilizzo del laboratorio di informatica e della postazioni di lavoro

Rispetto a questo punto sono state definite alcune disposizioni sull'uso del laboratorio:

1. Le apparecchiature presenti nella scuola sono patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
4. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.

5. Nei laboratori è vietato utilizzare CD personali o altri dispositivi se non dopo opportuno controllo con sistema di antivirus aggiornato.
6. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente
7. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al team digitale
8. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI (sezione che riguarda, in particolar modo la SS di 1° grado)

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe.
La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; gli interventi che sono pianificati, anche all'interno di percorsi specifici, promossi e attivati nei laboratori PON.
La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che gli alunni vivono: ***i docenti,*** in particolare, sono chiamati a essere anche *torre di avvistamento*, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che gli adolescenti possono vivere e affrontare ogni giorno. La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Equipe Pedagogica o Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

5.1 PREVENZIONE.

5.1.a. Rischi

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto del telefono cellulare personale o dello smartphone e dei pc della scuola collegati alla Rete.
Il telefono cellulare o lo smartphone non sono richiesti dalla scuola perché non sono ritenuti indispensabili in ambito scolastico, ma vengono forniti dai genitori degli alunni soprattutto per mantenere la comunicazione diretta con i figli anche fuori dal contesto scolastico. Talvolta, eludendo la sorveglianza dei docenti, attraverso i telefoni cellulari o gli smartphone, dotati di particolari applicazioni e di collegamento alla Rete, è possibile incorrere in rischi, per evitare i quali sono state previste alcune azioni.

5.1.b. Azioni.

Le azioni di prevenzione previste nell'utilizzo delle TIC sono:
1) Informare e formare docenti, genitori, personale ATA e alunni sui rischi che un uso non sicuro delle tecnologie digitali può favorire.
2) 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 di eventuali foto, immagini, testi e disegni relativi al/la proprio/a figlio/a).
3) Non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a comunicazioni urgenti 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.

4) Consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell'insegnante, che si accerta preventivamente dell'identità dell'interlocutore.
5) Utilizzare filtri e software che impediscano il collegamento a siti web per adulti (black list).

Le azioni di contenimento degli incidenti previste sono le seguenti:
1) Se la condotta incauta dell'alunno consiste nel fare circolare immagini imbarazzanti in Rete, è necessario contattare il service provider e se il materiale postato viola i termini e le condizioni d'uso del sito, chiedere di rimuoverle.
2) Suggerire di modificare i dettagli del profilo posizionandolo su *privato*, in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messengers, siti Social Network, Skype etc.), o suggerirgli di bloccare o ignorare particolari mittenti.
3) In caso di offese, 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 o, se necessario, cambiare il numero di cellulare contattando l'operatore telefonico.
4) Cancellare il materiale offensivo dal cellulare facendo intervenire i genitori e chiedere agli studenti di indicare a chi e dove lo hanno spedito per consigliarlo anche ad altri, conservando una copia di detto materiale, se necessario, per ulteriori indagini.
5) Contattare la Polizia Postale se si ritiene che il materiale offensivo sia illegale. In caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò è reato per chiunque.

5.2 RILEVAZIONE.

5.2.a. Che cosa segnalare.

Gli alunni 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, anche per fatti accaduti al di fuori della scuola. Confrontandosi periodicamente sui rischi delle comunicazioni *on line*, gli alunni possono riferire di fatti o eventi (personali o altrui) che *allertano* il docente.

5.2.b. Come segnalare: quali strumenti e a chi.

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.
Gli insegnanti, 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 l'alunno, usando il computer, si sta servendo di un servizio di messaggeria istantanea, programma che permette di chattare in linea tramite testo, l'insegnante può copiare, incollare e stampare la conversazione. Per gli eventuali collegamenti non autorizzati a siti Social Network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su 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 alunni, al Dirigente scolastico e per le condotte criminose alla Polizia.
La segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un alunno.
Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:
a) Annotazione del comportamento sul Registro e comunicazione scritta ai genitori, che la devono restituire vistata.
b) Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti.
c) 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 alunni la scelta di richiedere la punizione del colpevole, attraverso la querela.
Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).
In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

5.3 GESTIONE DEI CASI.

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

Gestione dei casi di "immaturità"

Può sembrare naturale all'alunno fornire i propri dati sui siti allestiti in modo tale da attrarre l'attenzione di coetanei, 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 dell'alunno e dall'altra dei molteplici messaggi espliciti che gli giungono quotidianamente attraverso i media (televisione, Internet, giornali e riviste), i discorsi degli altri bambini 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 tratteggiabili 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 *Cyberbullying* le molestie sono attuate mediante strumenti tecnologici:
a) invio di sms, messaggi in chat, e-mail offensive o di minaccia;
b) diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o email nelle mailing-list o nelle chat-line;
c) pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata;

Il bullismo in particolare può originarsi anche dall'esasperazione di conflitti presenti nel contesto scolastico. Il conflitto 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).
In considerazione dell'età degli alunni considerati possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il bullismo, i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli alunni.
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 alunni, 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 alunni 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 alunni 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).

I DOCENTI REFERENTI

Antonia Mellone

Mariagrazia Palmisano

IL DIRIGENTE SCOLASTICO

prof.ssa Concetta Patianna

ALLEGATI

MODULO DI RICHIESTA PER L'ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E PER L'UTILIZZO DEI DISPOSITIVI ELETTRONICI

Al Dirigente Scolastico
IC "San G. Bosco" Massafra –TA -

Il/La sottoscritto/a _____,nato/a a_____ (____), il _____, residente a_____ in via _____, n. _____ CAP _____ email _____ in qualità di genitore dell'alunno_____, iscritto/a alla classe _____ sez. _____ della Scuola _____ di _____:

Dichiara di essere consapevole delle implicazioni di responsabilità personale derivanti dall'accesso alla Rete Internet e dell'uso del cellulare e degli 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 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 o altri software malevoli all'interno della rete e a dare immediato avviso all'Amministrazione della Rete di comportamenti anomali o di infezioni riconosciute;
- non utilizzi il cellulare o altri dispositivi elettronici personali a scuola se non autorizzato dal docente;
- partecipi con impegno agli interventi educativi della scuola sulle modalità di utilizzo sicuro e consentito dei dispositivi elettronici e di Internet.

Data _____

Firma leggibile _____

DICHIARAZIONE LIBERATORIA DEI GENITORI/TUTORI PER LA PUBBLICAZIONE DI ELABORATI, NOMI, VOCI, IMMAGINI, MATERIALE AUDIOVISIVO

Al Dirigente Scolastico
IC "San G. Bosco" Massafra –TA -

I sottoscritti:

_____,nato/a a_____ (____), il _____, residente a_____ in via _____, n. _____ CAP _____ email _____

_____,nato/a a_____ (____), il _____, residente a_____ in via _____, n. _____ CAP _____ email _____

genitori/tutori dell'alunno_____, iscritto/a alla classe _____ sez. _____ della Scuola _____ di _____ :

- autorizzano l'IC "San G. Bosco" Massafra (TA) 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, …) del/la proprio/a figlio/a anche, se del caso, mediante riduzioni e/o adattamenti;
- dichiarano di essere informati che detto materiale potrà essere utilizzato per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto, pubblicazioni, cd-rom, mostre, seminari, convegni e altre iniziative promosse dalla scuola anche in collaborazione con altri soggetti;
- dichiarano 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;
- dichiarano che le suddette autorizzazioni/dichiarazioni hanno validità per l'intero ciclo della Scuola Secondaria di Primo grado, salvo eventuale successiva revoca.

Allegato: Fotocopie dei documenti di identità

Data _____

Firma _____

Firma _____

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, sempre più 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 prepotenze o in cui la vittima viene denigrata.

La rilevazione diretta degli indicatori da parte degli insegnanti o indiretta, sulla base di quanto riferito dagli alunni 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, alunni e genitori. Non serve, se non in casi particolarmente gravi, l'opera di psicologi, assistenti sociali, o altri specialisti a cui orientare la famiglia (Consultorio Familiare , Neuropsichiatria Infantile). L'elemento fondamentale per una buona riuscita del programma è infatti la corretta ristrutturazione del contesto relazionale degli alunni.

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 ALUNNI

1)Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere e caratteri speciali.
2) Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola.
3) Non inviare a nessuno fotografie tue o di tuoi amici.
4) Prima di inviare o pubblicare su un Blog la fotografia di qualcuno, chiedi sempre il permesso.
5) Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti dalla Rete.
6) Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola.
7) Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro.
8) Non rispondere alle offese ed agli insulti.
9) BLOCCA I BULLI: molti Blog e siti Social Network ti permettono di segnalare i *cyberbulli*.
10) Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto.
11) Se ricevi materiale offensivo (email, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di *cyberbullismo*.
12) Rifletti prima di inviare: ricordati che tutto ciò che invii su Internet diviene pubblico e rimane PER SEMPRE.
13) Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet.

14) Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori.
15) Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.
16) Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo insegnante o ai tuoi genitori prima di inviare messaggi.
17) Non scaricare (*download*) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori. 18) Non caricare (*upload*) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

LINEE GUIDA PER INSEGNANTI

1) Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune.
2) 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.
3) Discutete con gli alunni 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.
4) Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica e informate gli alunni che le navigazioni saranno monitorate.
5) Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione in Rete del Laboratorio (qualora sia stata attivata).
6) Ricordate agli alunni che la violazione consapevole della e-Safety Policy della scuola comporta sanzioni di diverso tipo.
7) Adottate provvedimenti disciplinari, proporzionati all'età e alla gravità del comportamento.
8) Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ridefinizione 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.
9) 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, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).
10) Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indizzo e-mail, ecc.
11) Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro.
12) 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

Consigli generali

1) Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia.
2) Evitate di lasciare le e-mail o file personali sui computer di uso comune.
3) Concordate con vostro figlio le regole: quando si può usare Internet e per quanto tempo.
4) Inserite nel computer i filtri di protezione: prevenite lo *spam*, i *pop-up* pubblicitari, l'accesso a siti pornografici.
5) Aumentate il filtro del *parentalcontrol* attraverso la sezione sicurezza in Internet dal pannello di controllo.
6) Attivate il *firewall* (protezione contro *malaware*) e antivirus.
7) Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona Internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante.

8) Incoraggiate le attività on line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi *amici* nel mondo.
9) Partecipa alle esperienze on line: naviga insieme a tuo figlio, incontra amici on line, discuti gli eventuali problemi che si presentano.
10) Comunicate elettronicamente con vostro figlio: inviate, frequentemente, e-mail, InstantMessage.
11) Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone.
12) Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia).
13) Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus.
14) Raccomandate di non scaricare file da siti sconosciuti.
15) Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate.
16) Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie.
17) Spiegate a vostro figlio 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 ad alcuno.
18) Spiegate a vostro figlio 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.
19) Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

Consigli in base all'età

Se tuo figlio ha meno di 8 anni:

1) Seleziona con molta attenzione i siti *sicuri*: ricordati che i gestori dei siti, per trarre il massimo guadagno, permettono agli inserzionisti di pubblicizzare i propri prodotti;
2) Comunica a tuo figlio tre semplici regole:
a) non dare il tuo vero nome, indirizzo e numero di telefono. Usa sempre il tuo *username* o *nickname*;
b) se compare sullo schermo qualche messaggio o *banner*, chiudilo: insegna a tuo figlio come si fa;
c) naviga esclusivamente sui siti autorizzati dai genitori: se vuoi andare su un nuovo sito, dobbiamo andarci INSIEME (molti siti richiedono la registrazione. Insegna a tuo figlio come registrarsi senza rivelare informazioni personali).

Se tuo figlio ha tra gli 8 anni e i 10 anni

1) Progressivamente diminuisci la supervisione: dagli otto ai dieci anni permetti a tuo figlio di navigare da solo nei siti autorizzati, sottolineando che deve consultarti prima di esplorarne dei nuovi.
2) Verifica periodicamente i contenuti dei siti *sicuri*.
3) Discuti con tuo figlio i rischi che possono presentarsi durante la navigazione on line; controlla, dalla *Cronologia* il menu navigazione, se tuo figlio ha consultato siti non autorizzati per i quali non ti ha chiesto il permesso.
4) Supervisiona l'email di tuo figlio dopo averlo reso consapevole del fatto che hai pieno accesso alle sue comunicazioni.
5) Se tuo figlio vuole usare Istant Messaging (IM) verifica che i suoi contatti siano limitati agli amici conosciuti.
6) Specifica che non può inserire nuovi contatti senza averti prima consultato.
7) Comunicagli che è assolutamente vietato cliccare su un link, contenuto in una email, su un *pop-up* pubblicitario o su un *banner* (ricordati, infatti, che potrebbero presentarsi immagini pornografiche o che potrebbe avviarsi il download di *malware*).
8) Incoraggia l'uso di Internet per svolgere ricerche scolastiche.
9) Definisci il tempo massimo di connessione ed incoraggia le attività con il mondo reale.

Se tuo figlio ha tra gli 11 anni e i 13 anni

Tuo figlio è diventato grande e potrebbe dirti che il suo migliore amico ha la possibilità di navigare tutti i giorni a tutte le ore. Che fare?

1) Crea una *partnership* con i genitori dei migliori amici di tuo figlio in modo da concordare con loro le regole: tempi di connessione, fasce orarie, siti autorizzati, modalità di utilizzo di IM.
2) Aiuta tuo figlio a creare una rete on line sicura: siti controllati ed amici conosciuti.

Se tuo figlio ha oltre 13 anni

1) Verifica i profili di tuo figlio e dei suoi amici, nei siti cerca persona, informandolo dei tuoi 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: condividi con tuo figlio le procedure per navigare in sicurezza ed evitare *on line* ed *off line* brutti incontri.
2) Confrontati con tuo figlio su tutti questi rischi e se protesta per il controllo, ribadisci che è un dovere del genitore supervisionare e monitorare l'uso di Internet.
3) Stringi un accordo: se tuo figlio dimostra di avere compreso i rischi e di sapere e volere usare Internet in modo sicuro, diminuisci la supervisione.
4) Il computer deve rimanere in salone o in una stanza accessibile a tutta la famiglia e non nella camera di tuo figlio ALMENO fino ai 16 anni.

PROTOCOLLI SIGLATI CON LE FORZE DELL'ORDINE E I SERVIZI DEL TERRITORIO PER LA GESTIONE CONDIVISA DEI CASI.

Non vi sono protocolli siglati ma forme ricorrenti di collaborazione nella prevenzione e contrasto del *bullismo* e del *cyberbullimo* da parte dell'Ente Locale, dello Sportello Amico, del Comando dei Carabinieri, della Polizia Posatale e di associazioni.

I docenti Referenti:

Antonia Mellone

Mariagrazia Palmisano

IL DIRIGENTE SCOLASTICO

Prof.ssa Concetta Patianna

Delibera n° 4 del CdD del 14/03/2018
Delibera n° 4 del CdI del 14/03/2018