ISTITUTO COMPRENSIVO STATALE"M.BUONOCORE - A.FIENGA"
Scuola dell'Infanzia – Primaria – Secondaria 1°Grado
80062 META (NA) - Via G.Marconi, 21
tel.081 8786997-fax.081 5323533 -C.M. NAIC871003 - C.F. 82019520632 – Distr. 039
E-mail : naic871003@istruzione.it E-mail PEC : naic871003@pec.istruzione.it
Sito Web : www.icbuonocorefiengameta.gov.it

E-Safety Policy

anno scolastico 2016 / 2017

1. INTRODUZIONE

1.1 Scopo della Policy di e-Safety

Lo scopo della e-Safety Policy è di stabilire i principi fondamentali tipici di tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie, affinchè Internet diventi lo strumento sia per condurre in modo più efficiente le funzioni amministrative e sia per svolgere esperienze formative, offrendo infinite opportunità per fare ricerca, comunicare, documentare il proprio lavoro, pubblicare elaborati e mettere in comune esperienze.

La Policy deve tendere a:

- salvaguardare e proteggere i bambini, i ragazzi e il personale tutto dell'Istituto;
- consentire al personale della scuola di lavorare in modo sicuro e responsabile con altre tecnologie di comunicazione di Internet e monitorare i propri standard e le prassi;
- impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo;
- affrontare eventuali casi di abuso on-line come il cyerbullismo, secondo regole comportamentali definite dalla scuola;

- garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

Le principali aree di rischio per la nostra comunità scolastica sono le seguenti:

- l'esposizione a contenuti on-line inappropriati oppure non autentici, ma ritenuti tali dagli alunni;
- il grooming, ovvero l'adescamento;
- il bullismo on-line in tutte le sue forme;
- la divulgazione di informazioni e di immagini personali; il sexting;
- il danneggiamento della reputazione on-line;
- l'incidenza negativa sulla salute e sul benessere degli individui (quantità di tempo speso on-line su Internet o giochi);
- l'assunzione e la diffusione di un'ideologia estremista;
- la poca cura o considerazione per i diritti d'autore relativamente a musica e film (copyright).

1.2 Ruoli e Responsabilità

(che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)

RUOLO	***RESPONSABILITA'***
Il Dirigente Scolastico	• vigilare sulla sicurezza dei dati; • garantire che la scuola utilizzi un Internet Service conforme ai requisiti di legge vigenti; • assicurare che il personale tutto riceva una informazione adeguata per svolgere i ruoli di sicurezza on-line e una specifica formazione per figure preposte; • promuovere le procedure da seguire in caso di infrazione della E-Safety Policy;

	• assumere un ruolo di primo piano nello stabilire e rivedere la E-Safety Policy.
I responsabili della sicurezza on-line (DSGA e docenti su nomina del DS)	• promuovere la consapevolezza e l'impegno per la salvaguardia on-line in tutta la comunità scolastica; • sensibilizzare i docenti ad inserire tematiche legate alla sicurezza on-line nei programmi di studio; • garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza on-line; • garantire che sia tenuto un registro sugli incidenti di sicurezza on-line ("Diario di bordo"); • facilitare la formazione e la consulenza per tutto il personale; • favorire il coordinamento con le autorità locali e le agenzie competenti in merito ad azioni bullismo e cyberbullismo; • favorire il controllo sulla diffusione impropria di dati personali.
L'Animatore Digitale, il team digitale e figure di sistema individuate dal referente	• pubblicare la E-Safety Policy sul sito della scuola; • diffondere la E- Safety Policy attraverso schede semplificative; • garantire che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati.
Gli insegnanti	• inserire tematiche legate alla sicurezza on-line nel programma di studi e di altre attività scolastiche; • supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia on-line; • garantire che gli alunni siano pienamente consapevoli delle capacità di ricerca e siano pienamente consapevoli dei problemi legali relativi ai contenuti elettronici come ad esempio le leggi sul copyright.

Il personale scolastico	• comprendere e contribuire a promuovere le politiche di e-Safety; • essere consapevoli dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili; • controllare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi; • segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza on-line; • usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; • garantire che le comunicazioni digitali con gli studenti avvengano a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio -mail, telefoni cellulari, salvo deroghe in casi eccezionali.
Gli alunni	• leggere, comprendere ed accettare la E- Safety Policy; • avere una buona comprensione delle capacità di ricerca on-line e della necessità di evitare il plagio e di rispettare le normative sul diritto d'autore; • capire l'importanza di segnalare abusi, o l'uso improprio o l'accesso a materiali inappropriati; • sapere quali azioni intraprendere se essi stessi o altri che conoscono si sentono preoccupati o vulnerabili quando si utilizza la tecnologia on-line; • conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili; • conoscere e capire la politica della scuola sull'uso di immagini e sul cyberbullismo;

	• capire l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali fuori dalla scuola; • assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa.
I genitori	• sostenere la scuola nel promuovere la sicurezza on-line e approvare l'accordo di E- Safety Policy con la scuola; • leggere, comprendere e controfirmare il suddetto accordo (Patto di Corresponsabilità); • accedere al sito web della scuola in conformità con quanto stabilito dalla stessa; • confidare che la scuola abbia preso tutte le precauzioni necessarie circa un uso corretto della tecnologia da parte degli alunni.

Al fine di garantire una gestione il più possibile corretta, Il **Dirigente Scolastico** garantisce di limitare l'accesso e l'uso della rete interna (Intranet) ed esterna (Internet) secondo i normali canali di protezione presenti nei sistemi operativi e favorisce un sistema per evitare comportamenti che non rientrano nelle norme che il Collegio dei Docenti delinea in proposito, come:

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

1.3 Disposizioni, comportamenti, procedure

- La scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina.
- La scuola archivia i tracciati del traffico Internet.
- E' vietato installare e scaricare da Internet software non autorizzati.
- Le postazioni PC in ambiente Windows sono protette da software che impediscono modifiche ai dati memorizzati sul disco fisso interno.
- Al termine di ogni collegamento la connessione deve essere chiusa.
- Verifiche antivirus sono condotte periodicamente sui computer e sulle unità di memorizzazione di rete.
- L'utilizzo di CD, DVD e chiavi USB personali degli alunni deve essere autorizzato dal docente e solo previa scansione antivirus per evitare qualsiasi tipo di infezione alla rete d'Istituto.
- Il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto, sempre nell'ambito del presente regolamento e nel rispetto delle leggi vigenti.

1.4 Condivisione e comunicazione della Policy all'intera comunità scolastica

La E-Safety Policy d'Istituto si applica a tutti i membri della scuola, compreso il personale, gli studenti, i genitori, gli utenti della comunità, che ne hanno accesso.

Il Dirigente Scolastico regola il comportamento degli studenti e autorizza i membri del personale di imporre sanzioni disciplinari per il comportamento inadeguato. Questo è pertinente a episodi di cyberbullismo, o altri tipi di incidenti che possono danneggiare la sicurezza on-line.

La scuola si occuperà di tali incidenti all'interno di questa Policy, delle politiche di comportamento e anti-bullismo associati ed avrà il compito di informare i genitori di episodi di comportamento inappropriato di sicurezza on-line, che si svolgono all'interno della scuola.

La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della E-Safety Policy sul sito della scuola;

- accordo di utilizzo accettabile, discusso con gli studenti e i genitori, all'inizio dell'anno scolastico, tramite il Patto di Corresponsabilità, che sarà sottoscritto dalle famiglie e rilasciato alle stesse;
- accordo di utilizzo accettabile rilasciato al personale scolastico.

1.5 Gestione delle infrazioni alla E-Safety Policy

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line. Tuttavia, a causa della scala internazionale collegata ai contenuti Internet, alla disponibilità di tecnologie mobili ed alla velocità di cambiamento, non è possibile garantire che il materiale inadeguato non apparirà mai su un computer della scuola o su un dispositivo mobile. Né la scuola né l'autorità locale possono assumersi la responsabilità per il materiale accessibile o le conseguenze di accesso scorretto a Internet.

Al personale e agli alunni saranno date informazioni sulle procedure relative alle infrazioni in uso e alle eventuali sanzioni. Le suddette procedure includono:

- informare dell'accaduto il docente della classe, il docente responsabile della sicurezza on-line (o il DSGA), il Dirigente Scolastico;
- informare dell'accaduto i genitori o i tutori;
- ritirare i dispositivi personali utilizzati impropriamente all'interno della scuola e consegnare gli stessi al Dirigente Scolastico fino a fine giornata, con possibilità di ritiro solo da parte di un genitore o tutore o adulto delegato dalla famiglia;
- sospendere l'uso dei pc nei laboratori e in classe per un dato periodo;
- segnalare i casi alle autorità competenti.

Il docente responsabile della sicurezza on-line fungerà da primo punto di riferimento per qualsiasi reclamo. Qualsiasi lamentela personale di abuso sarà riferita al Dirigente Scolastico e/o suo collaboratore.

Denunce di bullismo on-line saranno trattate in conformità con la legge attuale. Reclami relativi alla protezione degli alunni saranno trattati in conformità alle procedure di protezione dei minori.

1.6 Monitoraggio dell'implementazione della Policy e suo aggiornamento

La E-Safety Policy si inserisce all'interno di altre politiche scolastiche, quali la politica di protezione dei minori, la politica anti-bullismo, la politica del benessere degli alunni a scuola.

La scuola ha due docenti referenti del Progetto Generazioni Connesse che, insieme ai responsabili della sicurezza on-line e del cyberbullismo, si prenderanno cura della revisione e/o aggiornamento della Policy sotto la supervisione del DS.

La E-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con tutti i membri dello Staff e con le FF.SS.

Nell'ambito della revisione della Policy, tutte le informazioni e le revisioni saranno memorizzate per eventuali controlli, sulla base del seguente documento:

Versione	1.0
Data	GG/MM/AA
Autore	• Nome dei docenti responsabili della sicurezza on-line • Nome dei due docenti referenti del Progetto *Generazioni Connesse*
Approvato dal Dirigente Scolastico	
Approvato dal Collegio Docenti	
Descrizione modifica	
Data della prossima revisione	GG/MM/AA

Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base del seguente documento:

Anno scolastico	***Numero di segnalazioni***	***Numero di infrazioni***	***Numero di sanzioni disciplinari***

2. FORMAZIONE E CURRICULO

Il Piano Nazionale Scuola Digitale (PNSD) ha l'obiettivo di modificare gli ambienti di apprendimento per rendere l'offerta formativa di ogni istituto coerente con i cambiamenti della società e con le esigenze e gli stili cognitivi delle nuove generazioni. Il PNSD, con valenza pluriennale, è quindi un'opportunità per innovare la Scuola, adeguando non solo le strutture e le dotazioni tecnologiche a disposizione dei docenti e dell'organizzazione, ma soprattutto le metodologie didattiche e le strategie usate con gli alunni in classe.

Il D.M. 851 del 27 ottobre 2015**,** in attuazione dell'art.1, comma 56 della legge 107/2015, ne ha previsto l'attuazione al fine di:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un *team* per l'innovazione digitale, che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'Animatore Digitale;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative.

2.1 Curricolo sulle competenze digitali per gli studenti

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza on-line come parte del curriculum scolastico.

Si impegna a sviluppare una serie di competenze e comportamenti adeguati all'età degli alunni, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding in occasione della Settimana del codice;
- sviluppare una serie di strategie per rendere gli alunni in grado di:
- valutare e verificare le informazioni prima di accettarne l'esattezza;
- essere a conoscenza che l'autore di un sito web/pagina web può avere un particolare pregiudizio;
- sapere come restringere o affinare una ricerca;
- comprendere quale sia il comportamento accettabile quando si utilizza un ambiente on-line, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;
- capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione;
- capire perché 'amici on-line' potrebbero non essere chi dicono di essere e comprendere perché dovrebbero fare attenzione all'interno di un ambiente on-line;
- capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e/o informazioni di contatto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- sapere di non poter scaricare alcun file - come i file musicali - senza autorizzazione;
- comprendere l'impatto di bullismo on-line, sexting, grooming e sapere come cercare aiuto se sono in pericolo;
- sapere come segnalare eventuali abusi tra cui il bullismo on-line e come chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie in Internet;
- utilizzare con consapevolezza Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche.

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

Nell'ambito del PNSD questa scuola ha previsto:

- la nomina e la formazione di un Animatore Digitale che come docente accompagnerà il Dirigente Scolastico e il Direttore S.G.A. nell'attuazione degli obiettivi e delle innovazioni previste dal PSND;
- la formazione dei docenti in ingresso all'utilizzo del registro elettronico e dello scrutinio elettronico;
- la somministrazione di un questionario rivolto ai docenti per la rilevazione dei bisogni formativi "digitali";
- l'implementazione della connessione Internet nei plessi dell'Istituto;
- la ricognizione e la messa a punto delle dotazioni digitali;
- l'attivazione e la comunicazione di iniziative di formazione, in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale;
- l'assicurazione che il personale sappia come trattare dati sensibili o personali;
- l'offerta di corsi di formazione e/o aggiornamento a disposizione del personale in materia di TIC nella didattica e di sicurezza on-line;
- la trasmissione al nuovo personale delle informazioni e delle indicazioni in merito alla E-Safety Policy.

2.3 Sensibilizzazione delle famiglie

Questa scuola esegue un programma continuativo di consulenza, orientamento e formazione per i genitori, tra cui:

- presentare ai genitori, i cui figli si scrivono nel nostro Istituto, il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- pubblicare informazioni sul sito della scuola;
- offrire incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di sostegno per i genitori, come www.generazioniconnesse.it.

3. GESTIONE DELLE INFRASTRUTTURE E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

3.1 Accesso ad Internet: filtri ed antivirus

L'Istituto attualmente è dotato di una rete LAN cui accedono i computer dell'amministrazione/dirigenza, protetta da sw proprietari per quanto riguarda le connessioni con l'esterno, e di una rete LAN che permette la connessione ad Internet di tutte le LIM presenti nelle classi e nei vari laboratori (rete didattica); inoltre è presente una rete wireless destinata all'utilizzo didattico dei tablet nei vari ambienti scolastici; le password di accesso sono inserite automaticamente, ma non conosciute dalla platea scolastica.

Risulta necessario per tutta la comunità scolastica mantenere aggiornati gli antivirus su tutte le macchine e controllare i dispositivi di archiviazione esterna che vengono collegati al proprio PC (pen drive, DVD, ecc.).

Pertanto nel mese di settembre, prima dell'inizio dell'anno scolastico, sarà cura del responsabile contattare il tecnico informatico affinché si proceda all'aggiornamento suddetto.

Per quanto riguarda la rete amministrativa, lo storage è garantito da un backup automatico su altra postazione, mentre la rete didattica non prevede ancora un'archiviazione centrale di memorizzazione dati né alcun servizio di backup.

3.2 Gestione accessi

Ciascun utente connesso alla rete dovrà rispettare il presente regolamento, tutelare 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 l'insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete.

I genitori saranno invitati a firmare il contratto formativo nel quale sono presenti tali norme di comportamento e gli alunni dovranno impegnarsi a rispettare le indicazioni di buon utilizzo che la scuola si impegna a redigere e a divulgare attraverso il regolamento d'Istituto presente sul sito web, prima che sia concesso loro l'accesso a Internet.

3.3 E-mail

Non si pubblicano indirizzi di posta elettronica personali degli alunni o del personale sul sito della scuola.

L'Istituto comunica circolari, avvisi e altre notizie attraverso la sua casella di posta elettronica naic871003@istruzione.it a tutto il personale docente e ATA (ciascuno ha comunicato in segreteria il proprio indirizzo e-mail) e le comunicazioni ai genitori (compiti, eventuali note, valutazioni quadrimestrali) avvengono tramite il software utilizzato dall'Istituto per il registro elettronico.

Le comunicazioni tra personale scolastico e famiglie via e-mail devono avvenire preferibilmente tramite l'indirizzo e-mail della scuola, 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

L'Istituto dispone di un proprio spazio web e di un proprio dominio: www.icbuonocorefiengameta.gov.it

La gestione del sito della scuola, la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione, sono a cura del collaboratore amministrativo competente.

La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per cui è stato chiesto ed ottenuto il permesso dall'autore proprietario.

Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.

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

4. STRUMENTAZIONE PERSONALE

4.1 Per gli studenti

Come da regolamento d'Istituto agli alunni è vietato l'utilizzo dei cellulari all'interno della scuola. Per quanto concerne l'utilizzo dei tablet, questi possono essere utilizzati solo alla presenza del docente e per motivi strettamente scolastici.

4.2 Per il personale della scuola

I docenti ed il personale della scuola possono utilizzare cellulari e tablet a scopo personale non durante l'attività didattica o lavorativa.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1 Prevenzione

- 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 altrui, dello smartphone personale o altrui, dei pc della scuola collegati alla rete.

Il telefono cellulare e 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 fuori dal contesto scolastico. Eludendo la sorveglianza degli insegnanti, attraverso i telefoni cellulari o gli smartphone, dotati di particolari applicazioni e di collegamento a Internet, oltre che parlare e scrivere messaggi con i genitori o terzi, gli alunni potrebbero anche scaricare e spedire foto personali o intime, proprie altrui, video con contenuti indecenti o violenti, accedere a Internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc dei laboratori e con un accesso non controllato a Internet.

- Azioni

Le azioni previste per la prevenzione nell'utilizzo delle TIC sono le seguenti:

- ❖ informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire;
- ❖ fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a);
- ❖ non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto, per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci, è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino;
- ❖ consentire l'utilizzo del cellulare solo in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico, durante una visita guidata, e comunque sotto la supervisione dell'insegnante;
- ❖ utilizzare software che impediscono il collegamento ai siti web a rischio;
- ❖ centralizzare il blocco dei siti web sul server del docente, utilizzando software che possono bloccare l'accesso ai siti Internet semplicemente esaminando le varie richieste di connessione provenienti dai client collegati in rete locale, in modo tale che, anche indipendentemente dal browser in uso su ciascuna macchina, il software sia capace di intercettare le richieste di collegamento e rigettare quelle che non rispettano le regole imposte dall'amministratore.

Le azioni di contenimento degli incidenti previste sono le seguenti:

- ➢ se la condotta incauta dell'alunno consiste nel fare circolare immagini imbarazzanti, di natura sessuale, su Internet, è necessario rimuoverle: contattare il service provider e se il materiale postato viola i termini e le condizioni d'uso del sito chiedere di rimuoverle;
- ➢ se l'alunno viene infastidito od offeso, suggerirgli di modificare i dettagli del proprio profilo sistemandolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messengers, siti social network, Skype etc.), o suggerirgli di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici con i quali regolarmente chatta, di inserire il compagno o la persona che offende, per quanto riguarda l'e-mail, tra gli indesiderati;
- ➢ consigliare di cambiare il proprio indirizzo e-mail, contattando l'e-mail provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o, se necessario, cambiare il numero di cellulare contattando l'operatore telefonico;

- fare cancellare il materiale offensivo dal telefonino, facendo intervenire i genitori, e chiedere agli studenti di indicare a chi e dove lo hanno spedito per farlo fare anche gli altri, e conservare una copia di detto materiale, se necessario, per ulteriori indagini;
- contattare la polizia se si ritiene che il materiale offensivo sia illegale; in caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò è reato per chiunque.

5.2 Rilevazione

- 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. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni on-line, i minori possono riferire fatti o eventi personali o altrui che "allertano" l'insegnante.

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

I contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola attualmente dai minori (l'eventuale telefonino/smartphone personale e il pc collegato ad Internet) per gli alunni possono essere i seguenti:

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

video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

- Come segnalare: quali strumenti e a chi.

- ❖ Per il 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.

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

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

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

- ➢ annotazione del comportamento sul registro elettronico e comunicazione scritta ai genitori, che la devono restituire vistata;
- ➢ convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- ➢ 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 ad 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

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

5.3.1 Gestione dei casi di "immaturità"

Può sembrare naturale all'alunno fornire i propri dati personali su siti allestiti in modo tale da attrarre l'attenzione di bambini e ragazzi, 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, DVD, Internet, giornali e riviste), i discorsi degli altri bambini e/o ragazzi o degli adulti.

I comportamenti cosiddetti "quasi aggressivi", che spesso si verificano tra coetanei, le interazioni animate, 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 la 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 e di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

5.3.2 Gestione dei casi di “prepotenza” o “prevaricazione”

I comportamenti definibili come atti di “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 sia da un solo soggetto sia da un gruppo.

Nel caso particolare del Cyberbullismo le molestie sono attuate attraverso strumenti tecnologici:

- invio di sms, messaggi in chat, e-mail offensive 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.

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 non lo si gestisce in un’ottica evolutiva dei rapporti, di negoziazione e di 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 dunque i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli allievi.

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 dal team dei docenti della classe, 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 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" e insegnare ad opporvisi, per far acquisire da un lato fiducia nelle proprie sensazioni e nel proprio intuito e dall'altro 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, 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).

5.3.3 Gestione degli "abusi sessuali"

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

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

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

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

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

Il compito della scuola non si riduce solo alla "segnalazione", ma è più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare l'alunno a riprendere una crescita serena.

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

6. ANNESSI **(da prodursi a cura della scuola)**

6.1 Procedure operative per la gestione delle infrazioni alla Policy

Il MODULO DI RICHIESTA PER L'ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E PER L'UTILIZZO DEI DISPOSITIVI ELETTRONICI e il MODULO DI RICHIESTA DI CREDENZIALI DI AUTENTICAZIONE/DI ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E DI UTILIZZO DEI DISPOSITIVI ELETTRONICI non sono stati ancora prodotti e si provvederà ad inserirli al primo aggiornamento della Policy.

6.2 Procedure operative per la protezione dei dati personali

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

Al Dirigente Scolastico

dell'Istituto Comprensivo "Buonocore – Fienga"

Meta (Na)

Oggetto:Liberatoria per l'utilizzo delle immagini.

Dati dell'Alunno

Cognome _____Nome_____
nato/a_____il_____
Scuola_____classe_____sez._____

Dati del genitore

_L_sottoscritt_____
nato/a_____il_____

con la presente **AUTORIZZA** l'utilizzo delle immagini registrate nell'ambito delle attività/progetti realizzati dall'istituzione Scolastica, con diffusione sulle piattaforme digitali e in televisione, nel pieno rispetto della funzione educativa degli interventi. La posa e l'utilizzo delle immagini sono da considerarsi effettuate in forma gratuita.

Firma del genitore

_____

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

6.3.1 CYBERBULLISMO: alcuni campanelli di allarme

Gli atti di bullismo avvengono prevalentemente entro o nei dintorni del contesto scolastico, tuttavia in misura crescente le prepotenze vengono riportate nel contesto virtuale di Internet. In queste situazioni si parla di cyberbullismo 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 denigrate.

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: insegnanti e altro personale scolastico, alunni e genitori. Non serve, se non in casi particolarmente gravi, l'opera di psicologi, assistenti sociali, o altri specialisti verso cui orientare la famiglia. L'elemento fondamentale per una buona riuscita del programma è infatti la corretta ristrutturazione del contesto relazionale degli alunni.

6.3.2 ABUSI SESSUALI: alcuni campanelli di allarme

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

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

A chi segnalare:

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

E' fondamentale non operare in modo isolato, ma confrontarsi con i colleghi di classe e il Dirigente Scolastico.

6.4 Procedure operative per la gestione dei casi.

6.4.1 LINEE GUIDA PER ALUNNI

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere e caratteri speciali;
- mantieni segreto il tuo nome, l'indirizzo e il telefono di casa, il nome e l'indirizzo della tua scuola;
- non inviare a nessun fotografie tue o di tuoi amici;
- prima di inviare o pubblicare su un Blog la fotografia di qualcuno, chiedi sempre il permesso;
- chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet;
- chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola;
- quando sei connessi alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
- non rispondere alle offese ed agli insulti;
- blocca i Bulli: molti Blog, siti e social network ti permettono di segnalare i cyberbulli;
- conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;

- se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali), non diffonderlo: potresti essere accusato di cyberbullismo;
- rifletti prima di inviare: ricordati che tutto ciò che invii su Internet diviene pubblico e rimane per SEMPRE;
- riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non risponder mai; inoltre riferisci al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
- se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori;
- ricordati che le persone che incontri nella rete sono degli estranei e non sempre sono quello che dicono di essere;
- non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo insegnante prima di inviare messaggi dalla scuola o rivolgiti ai tuoi genitori prima di inviare messaggi da casa;
- non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori;
- non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

6.4.2 LINEE GUIDA PER INSEGNANTI

- Evitate di lasciare e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
- salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali;
- discutete con gli alunni della e-safety policy della scuola, dell'utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate;
- ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
- ricordate agli alunni che la violazione consapevole della e-safety policy della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo;

- adottate provvedimenti “disciplinari”, proporzionati all’età e alla gravità del comportamento;
- adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell’eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni;
- nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi (sportello di ascolto psicologico gratuito attualmente attivo presso la scuola, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica - Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
- chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc...;
- segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro;
- in caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come Internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all’autorità giudiziaria o agli organi di Polizia.

6.4.3 CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

6.4.3.1 Consigli generali

- Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia;
- evitate di lasciare le e-mail o file personali sui computer di uso comune;
- concordate con vostro figlio le regole: quando si può usare Internet e per quanto tempo...
- inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l’accesso a siti pornografici;
- aumentate il filtro del “parental controll” attraverso la sezione sicurezza in Internet dal pannello di controllo;
- attivate il firewall (protezione contro malware) e antivirus;

- 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;
- incoraggiate le attività on-line di alta qualità: ricercate informazioni scientifiche, ricercate nuovi amici nel mondo;
- partecipate alle esperienze on-line: navigate insieme a tuo figlio, incontrate amici on-line, discutete sugli eventuali problemi che si presentano;
- comunicate elettronicamente con vostro figlio: inviate frequentemente e-mail, Instant Message;
- 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;
- stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);
- discutete sul tema dello scaricare file e della possibilità di ricevere file con virus;
- raccomandate di non scaricare file da siti sconosciuti;
- incoraggiate vostro figlio a dirvi se vede immagini particolari o se riceve e-mail indesiderate;
- discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie;
- spiegate a vostro figlio che le password, i codici PIN, i numeri di carta di credito, i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno;
- 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;
- il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

6.4.3.2 <u>Consigli in base all'età</u>

6.4.3.2.1. *Se vostro figlio ha meno di 8 anni*

- Selezionate con molta attenzione i siti "sicuri": ricordatevi che i gestori dei siti, per trarre il massimo guadagno, permettono agli inserzionisti di pubblicizzare i propri prodotti;

- Comunicate a vostro figlio tre semplici regole:

- "non dare il tuo vero nome, indirizzo e numero di telefono; usa sempre il tuo computer username o nickname";
- "se compare sullo schermo qualche messaggio o banner, chiudilo!" (insegnate a vostro figlio come si fa);
- "naviga esclusivamente sui siti autorizzati dai genitori: se vuoi andare su un nuovo sito, dobbiamo andarci INSIEME" (molti siti richiedono la registrazione: insegnate a vostro figlio come registrarsi, senza rivelare informazioni personali).

6.4.3.2.2 *Se vostro figlio ha tra gli 8 anni e i 10 anni*

- Progressivamente diminuite la supervisione: dagli otto ai dieci anni permettete a vostro figlio di navigare da solo nei siti autorizzati, sottolineando che deve consultarti prima di esplorarne dei nuovi.

- Verificate periodicamente i contenuti dei siti "sicuri".

- Discutete con vostro figlio i rischi che possono presentarsi durante la navigazione on-line.

- Controllate, dalla cronologia, il menu navigazione, per verificare se vostro figlio ha consultato siti non autorizzati per i quali non vi ha chiesto il permesso.

- Supervisionate l'e-mail di vostro figlio, dopo averlo reso consapevole del fatto che avete pieno accesso alle sue comunicazioni.

- Se vostro figlio vuole usare IM, verificate che i suoi contatti siano limitati agli amici conosciuti. Specificate che non può inserire nuovi contatti senza avervi prima consultato.

- Comunicategli che è assolutamente vietato cliccare su un link, contenuto in una e-mail, su un pop-up pubblicitario o su un banner (ricordatevi, infatti, che potrebbero presentarsi immagini pornografiche o che potrebbe avviarsi il download di "malware") .

- Incoraggiate l'uso di Internet per svolgere ricerche scolastiche.

- Definite il tempo massimo di connessione ed incoraggiate le attività con il mondo reale.

6.4.3.2.3 *Se vostro figlio ha tra gli 11 anni e i 13 anni*

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

Create una partnership con i genitori dei migliori amici di vostro figlio, in modo da concordare con loro le regole: tempi di connessione, fasce orarie, siti autorizzati, modalità di utilizzo di IM (messaggistica istantanea).

Aiutate vostro figlio a creare una rete on-line sicura: siti controllati ed amici conosciuti.

6.4.3.2.4 *Se vostro figlio ha oltre 13 anni*

Verificate i profili di vostro figlio e dei suoi amici, nei siti cerca persona, informandolo dei vostri periodici controlli.

Ricordatevi che in questa fascia di età aumentano le ricerche di materiale sessuale ed i rischi di seduzioni sessuali on-line da parte di cyberpredatori adulti: condividete con vostro figlio le procedure per navigare in sicurezza ed evitare, on-line ed off-line, brutti incontri.

Confrontatevi con vostro figlio su tutti questi rischi e se protesta per il controllo, ribadite che è un dovere del genitore supervisionare e monitorare l'uso di Internet.

Stringete un accordo: se vostro figlio dimostra di avere compreso i rischi e di sapere e volere usare Internet in modo sicuro, diminuite la supervisione.

Il computer deve rimanere in salone o in una stanza accessibile a tutta la famiglia e non nella camera di vostro figlio ALMENO fino ai 16 anni.

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

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

F.to il Dirigente Scolastico

dott.ssa Ester Miccolupi

Firma autografa sostituita a mezzo stampa, ai sensi dell'art. 3, comma 2 del D.Lgs. n. 39/1993