Generazioni Connesse
SAFER INTERNET CENTRE

Progetto co-finanziato
European Commission

Fondo Sociale Europeo

Istituto Comprensivo
"GIUSEPPE GRASSI"

Viale Stazione, 13 – 74015 MARTINA FRANCA (TA) – ITALY

Prot.n. 1770/C27 del 16/05/2017

E-Safety Policy

INDICE RAGIONATO
E-Safety Policy

1. Introduzione
- Scopo della Policy.
- Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*).
- Condivisione e comunicazione della Policy all'intera comunità scolastica.
- Gestione delle infrazioni alla Policy.
- Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo
- Curricolo sulle competenze digitali per gli studenti.
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- Sensibilizzazione delle famiglie.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.
- Accesso ad internet: filtri, antivirus e sulla navigazione.
- Gestione accessi (password, backup, ecc.).
- E-mail.
- Blog e sito web della scuola
- Social network.
- Protezione dei dati personali.

4. Strumentazione personale
- Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..
- Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..
- Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione
- Rischi
- Azioni

Rilevazione
- Che cosa segnalare
- Come segnalare: quali strumenti e a chi.
- Come gestire le segnalazioni.

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

Annessi (da prodursi a cura della scuola)
1. Procedure operative per la gestione delle infrazioni alla Policy.
2. Procedure operative per la protezione dei dati personali.
3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.
4. Procedure operative per la gestione dei casi.
5. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

1. Introduzione

- Scopo della Policy.

Il presente documento ha lo scopo di individuare norme comportamentali e procedure per l'utilizzo delle ICT nel nostro Istituto, nonché misure per la prevenzione e per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.
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,
- far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali,
- 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 minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.
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.
La nostra scuola ha aderito nel mese di settembre 2016 al progetto "Generazioni Connesse" e, dopo una prima fase di analisi dei fabbisogni e delle risorse del nostro Istituto, è stato stilato, nel mese di febbraio 2017, un Piano d'Azione individuando percorsi e risorse necessarie per elaborare e implementare una Policy di ESafety .
Si precisa che il progetto "Generazioni connesse" è stato inserito nel Piano Triennale dell'Offerta Formativa nell'area riguardante le fasi di attuazione del PNSD.
Il documento potrà essere revisionato annualmente.

- Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*).

1) Dirigente scolastico
Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

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

2) Animatore digitale
Il ruolo dell'Animatore digitale include i seguenti compiti:

- stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi;
- favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di coding per

tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

3) Direttore dei servizi generali e amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni
- curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

4) Docenti:

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni(ovvero valutazioni sulla condotta non adeguata degli stessi)rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

5) Allievi:

Il ruolo degli alunni include i seguenti compiti:

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

6) Genitori:

Il ruolo dei genitori degli alunni include i seguenti compiti:

- Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'Informazione e delle Comunicazioni nella didattica
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet
- Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet
- Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.

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

a) Condividere e comunicare la politica di e-safety agli alunni

- Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.
- Uno o più moduli di insegnamento sulla e-safety saranno programmati nell'ambito della disciplina "Tecnologia" per aumentare la consapevolezza e importanza di un uso sicuro e responsabile di internet tra gli alunni.
- L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete.
- L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet.
- Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

b) Condividere e comunicare la politica di e-safety al personale

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali (consigli di interclasse/intersezione, collegio dei docenti) e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web.
- Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali.
- Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato.
- Un'adeguata informazione/formazione on line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola.
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici.
- L'Animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con i bambini in classe. Questi strumenti varieranno a seconda dell'età e della capacità degli alunni.
- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

c) Condividere e comunicare la politica di e-safety ai genitori

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree 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, collegiali e individuali.
- L'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa.
- L'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.
- Il Comitato Genitori dell'Istituto collaborerà nelle attività di informazione/formazione degli alunni e dei genitori.

- Gestione delle infrazioni alla Policy.

1) Disciplina degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate (bambini e ragazzi di età fino ai 14 anni), sono prevedibilmente le seguenti:

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

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo del bambino. Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.
Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:
- il richiamo verbale
- il richiamo scritto con annotazione sul diario
- il richiamo scritto con annotazione sul registro
- la convocazione dei genitori da parte degli insegnanti
- la convocazione dei genitori da parte del Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli 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.

2) Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

3) Disciplina dei genitori

In considerazione dell'età dei bambini e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Le situazioni familiari meno favorevoli sono:
- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

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

- Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, del Team Digitale e dei docenti delle classi, tramite questionari e conversazioni.

Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.
L'aggiornamento della policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dagli Organi Collegiali, a seconda degli aspetti considerati.

- Integrazione della Policy con Regolamenti esistenti.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso efficace e consapevole del digitale nella didattica:
- PTOF, incluso il piano per l'attuazione del PNSD;
- POF;
- Regolamento interno d'istituto;
- Regolamento per l'utilizzo dei laboratori di informatica.

2. Formazione e Curricolo

- Curricolo sulle competenze digitali per gli studenti.

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 (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet".
Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. L'approccio per discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.
L'istituto ha inoltre aderito negli aa.ss. 2015/2016 e 2016/2017 al progetto ministeriale "Programma il futuro", sperimentandole attività di coding in molte delle classi presenti nella scuola ed integrando così le competenze ditali già previste dalle Indicazioni Nazionali, attraverso la promozione dello sviluppo negli alunni del "pensiero computazionale".

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

Il corpo docente ha partecipato estesamente a corsi di formazione nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete.
Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, può pertanto prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse

dall'Amministrazione centrale e dalle scuole polo; la partecipazione a corsi di aggiornamento online, può comprendere altresì la fruizione dei materiali messi a disposizione dall'Animatore.

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

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle ICT e di prevenire e contrastare "ogni forma di discriminazione e del bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto ha aderito, quest'anno, al progetto "Generazioni Connesse" (SIC ITALY II), coordinato dal MIUR, in partenariato col Ministero dell'Interno-Polizia Postale e delle Comunicazioni e con altre importanti associazioni per la tutela dei diritti dei minori, come Children Italia e Telefono Azzurro. Per la portata e il numero elevato di azioni che l'istituto si è impegnato a portare avanti nel Piano d'Azione redatto nel mese di marzo 2017, il progetto si estenderà al prossimo anno scolastico.
Sarà predisposta una bacheca online per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, collegata alla homepage del sito scolastico (www.istitutocomprensivograssi.gov.it), fruibile attraverso l'inserimento di una password cliccando sul link in homepage.

- Sensibilizzazione delle famiglie.

L' Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine saranno programmati 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.
Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni connesse" 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 darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

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

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

L'accesso a internet è possibile in tutte le aule collegandosi al wifi della scuola; sono previsti accessi diversi per gli studenti, per i docenti e per gli ospiti.
Nel laboratorio di informatica l'accesso alla rete è schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list o consentono il collegamento solo a siti idonei alla didattica.

- Gestione accessi (password, backup, ecc.).

L'accesso a internet è possibile in tutte le aule collegandosi al wifi della scuola; sono previsti accessi diversi per gli studenti, per i docenti e per gli ospiti.

Per fruire del laboratorio di informatica i docenti registrano l'accesso della classe, scrivendo su un registro la data e l'orario di utilizzo del laboratorio e il nominativo dell'alunno che utilizza la postazione numerata. Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

- E-mail.

L'account di posta elettronica istituzionale viene utilizzato ordinariamente dagli uffici amministrativi., sia per la posta in ingresso che in uscita.
La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

- Blog e sito web della scuola

La scuola attualmente ha un blog e un sito web.
Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione dell'Animatore digitale, che ne valuta con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.
L'Animatore Digitale è responsabile dell'aggiornamento periodico di tutti i canali di comunicazione digitale.

- Social network.

Attualmente nella didattica non si utilizzano social network.
L'istituzione scolastica ha creato una pagina Facebook col proprio profilo gestita dall'Animatore Digitale.

- Protezione dei dati personali.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).
Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori nonché richiesta di consenso ad effettuare riprese televisive, fotografie, interviste, pubblicazioni di elaborati, ecc a scopo di documentazione scolastica delle attività educative.

4. Strumentazione personale

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

In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola.
Non è consentito l'uso di dispositivi personali se non per utilizzi didattici in attività previste dai docenti.

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

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili. Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

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

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

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

- Rischi

I rischi più comuni che i ragazzi possono incorrere sul web riguardano tutti quei fenomeni legati al bullismo/cyberbullismo – una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali –; al sexting - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet (Levick& Moon 2010) – e all'adescamento o grooming – una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata (Glossario di "Generazioni connesse").
I rischi che i ragazzi possono correre a scuola nell'utilizzo di dispositivi digitali possono derivare principalmente da un uso non corretto del telefono cellulare o di altri dispositivi come lo smartphone o il tablet. Sebbene, infatti, l'uso del cellulare e dello smartphone non sia consentito dal Regolamento dell'Istituto, alcuni studenti potrebbero, anche in orario scolastico, violare il Regolamento e, eludendo la sorveglianza del personale della scuola, accendere ed adoperare il cellulare o lo smartphone, non solo per comunicare con i propri genitori, ma anche per navigare su internet, andando su siti non adatti e inviando materiali riservati (foto, video e altro).
Così facendo, gli studenti possono incorrere anche a scuola nei rischi sopra menzionati, entrando in contatto e persino in confidenza con sconosciuti, fino a ricevere messaggi molesti e adescamenti.

- Azioni

Le azioni previste di prevenzione nell'utlizzo 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.
- 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, che si accerta preventivamente dell'identità dell'interlocutore.
- Utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list)
- Centralizzare il blocco dei siti web sul server del docente, utilizzando software che possono bloccare l'accesso ai siti internet semplicemente esaminando le varie richieste di connessione provenienti dai client collegati in rete locale, in modo tale che anche indipendentemente dal browser in uso su ciascuna macchina, il software sia capace di intercettare le richieste di collegamento e rigettare quelle che non rispettano le regole imposte dall'amministratore.

Le azioni di contenimento degli incidenti previste sono le seguenti:
- Se la condotta incauta 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.

Rilevazione

- Che cosa segnalare

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 a internet) per gli alunni possono essere i seguenti:
- Contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.
Il docente è autorizzato a controllare le strumentazioni della scuola, per controllare l'uso del telefono cellulare di un alunno occorre rivolgersi al genitore.

- Come segnalare: quali strumenti e a chi.

Il personale della scuola, anche con l'ausilio dell'Animatore Digitale, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola; 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 consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi. Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso, il Dirigente scolastico e, ove si configurino reati, la Polizia Postale.
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 devono comunque essere comunicate ai genitori e al Dirigente scolastico; per quelle criminose, anche alla Polizia Postale.
Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto.

- Come gestire le segnalazioni.

In base all'entità dei fatti si provvederà:

1 . Comunicazione scritta tramite diario alle famiglie;

2. Nota disciplinare sul Registro di classe;
2 . Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
3 . Convocazione delle famiglie da parte del Dirigente scolastico.

Per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti o direttamente all'Autorità giudiziaria.

Gestione dei casi

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

a) Casi di cyberbullismo:

Si definiscono bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo.
Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online.
Tale specifica forma di bullismo ha caratteristiche peculiari:
1) è pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
2) è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
3) spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.
Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato ad esserne consapevole.

Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- informare i genitori degli alunni coinvolti;
- coinvolgere il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- tenere traccia di quanto successo e delle azioni intraprese in una relazione dettagliata per consentire ulteriori indagini se necessarie.

b) Casi di sexting:

Qualora ci si trovi di fronte a un caso di sexting (con cui si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite via cellulare o tramite internet) si dovrà:

- coinvolgere la classe e confrontarsi con esperti per capire come approfondire e affrontare il fenomeno;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al sexting;
- documentarsi opportunamente sulle norme giuridiche che regolano i comportamenti e le condotte sessuali in Italia;
- intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno ripone negli altri e sul fenomeno del sexting, approfondendo casi e testimonianze.

c) Casi di adescamento online o grooming:

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti "concedono" la loro amicizia non solo a persone che conoscono

direttamente, ma anche ad "amici di amici". Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali.
L'adescamento online (grooming) consiste nel tentativo, da parte di un adulto, di avvicinare un/a bambino/a o adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet (tramite chat, blog, forum e social networks, per esempio).In un primo tempo, l'adulto, spesso mentendo sulla propria identità e sulla propria età, mostra particolare interesse nei confronti del/la bambino/a o dell'adolescente, cercando di conquistarne la fiducia. Solo in un secondo tempo, cerca di entrare sempre più nell'intimità del bambino fino a introdurre argomenti intimi e attinenti alla sfera sessuale.
È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale.
Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico; un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo; allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti, ecc., è bene:
- approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- farsi affiancare da esperti, per offrire ai minori, qualora lo desiderino, il supporto necessario.

Annessi (da prodursi a cura della scuola)

6. Procedure operative per la gestione delle infrazioni alla Policy.
7. Procedure operative per la protezione dei dati personali.
8. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.
9. Procedure operative per la gestione dei casi.
10. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

1. Procedure operative per la gestione delle infrazioni alla Policy.

MODULO DI RICHIESTA DI CREDENZIALI DI AUTENTICAZIONE/DI ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E DI UTILIZZO DEI DISPOSITIVI ELETTRONICI

Al Dirigente Scolastico
I.C. G. GRASSI – Martina Franca

Il/La sottoscritto/a _____, nato/a a _____ (___), il _____, residente a _____ in via _____, n. _____ CAP _____ email _____ in qualità di docente/personale ATA (cancellare la voce che non interessa) in servizio presso la scuola _____ plesso _____,
chiede il rilascio delle credenziali di autenticazione /l'accesso ad Internet nella rete di Istituto.
Dichiara
- di aver letto e compreso il documento di "Policy e-safety", di utilizzo accettabile della rete internet, pubblicato sul sito della Scuola;
- di essere consapevole delle implicazioni di responsabilità personale derivanti dall'accesso alla rete internet e dagli eventuali abusi.
In particolare si impegna a
- non scaricare/duplicare/distribuire software o altri contenuti protetti da diritto d'autore;
- non accedere a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola (ad esempio, siti con contenuto violento, pedo-pornografico, razzista, etc…);
- non collegarsi ad internet a scopi commerciali o di profitto personale e per attività illegali;
- non diffondere 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;
- conservare le credenziali di accesso alla rete in modo scrupoloso, non comunicandole ad altre persone.
E' consapevole che l'accesso attraverso l'autenticazione trasferisce direttamente la responsabilità degli atti commessi durante la navigazione all'intestatario delle credenziali stesse.
Dichiara di essere consapevole che
-l'autorizzazione all'uso della rete di Istituto potrà venire revocata (cancellazione dell'utente) in qualsiasi momento per cause tecniche o per motivazioni legate all'uso improprio o alla violazione delle norme di comportamento;
-l'utilizzo dei dispositivi elettronici e della rete della scuola deve essere utilizzata per attività di servizio o funzionali alle stesse;
- l'utilizzo della rete per l'assunzione di impegni o responsabilità per conto della scuola deve essere autorizzata dal Dirigente scolastico, legale rappresentante dell'istituzione nonché legittimo titolare dell'utenza
- l'utilizzo del cellulare e di altri dispositivi elettronici personali a scuola deve avvenire nei limiti consentiti dalla legge e dai regolamenti dell'istituzione scolastica, in situazioni di necessità ed urgenza o per ragioni di servizio;
- ci si deve rivolgere per la necessaria assistenza alla connessione o al funzionamento dei dispositivi contattando l'Animatore digitale o il referente del laboratorio di informatica o gli uffici di segreteria, evitando tentativi incerti di ripristino o di modificazione delle impostazioni.

Data _____ Firma leggibile _____

DICHIARAZIONE DI CONSENSO AL TRATTAMENTO DEI DATI PERSONALI
(D. L.vo 196/2003 – CODICE DELLA PRIVACY)

Consapevole che in occasione di manifestazioni scolastiche, anche pubbliche, di presentazione delle attività didattiche svolte e/o di promozione degli scopi istituzionali della Scuola, potranno essere effettuate riprese televisive, fotografie, interviste, pubblicazione di elaborati, ecc., anche a scopo di documentazione scolastica e/o personale/familiare delle iniziative educative realizzate, con conseguente trattamento di dati personali anche sensibili, **dà/non dà il proprio consenso ed autorizza/non autorizza** l'I.C. "GRASSI" all'utilizzo degli stessi per articoli di stampa, trasmissioni radiotelevisive, per realizzazione del giornale di istituto, di mostre, di cartelloni, sul sito internet/blog della Scuola ed altri mezzi multimediali di pubblicizzazione/documentazione delle attività educative. Tale autorizzazione si intende gratuita e valida fino al completamento del corso di studi presso questo Istituto.

Firma _____

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

CYBERBULLISMO: alcuni campanelli di allarme
Gli atti di bullismo avvengono prevalentemente entro o nei dintorni del contesto scolastico, tuttavia in misura crescente le prepotenze vengono riportate nel contesto virtuale di internet.
In queste situazioni si parla di cyberbullying che si manifesta attraverso:
- invio di sms, mms, e-mail offensivi/e o di minaccia
- diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing-list o nelle chat-line
- pubblicazione nel cyberspazio di foto o filmati che ritraggono 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. Nei casi particolarmente gravi potrà essere richiesto l'intervento di psicologi, assistenti sociali, o altri specialisti a cui orientare la famiglia.

ABUSI SESSUALI: alcuni campanelli di allarme
Internet ha ampliato le possibilità di abuso sessuale dei minori infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile (pedopornografia) in cui le vittime sono appunto i minori. Inoltre succede che un adulto prenda contatto con dei bambini nei forum o nelle chat su internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i bambini a spogliarsi davanti alla webcam oppure a inviare una fotografia che li ritrae nudi tramite internet o sul cellulare. L'osservazione della presenza dei suddetti indicatori da parte degli insegnanti deve essere attenta e pronta alla segnalazione.

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

4. 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 da Internet.
6) Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola.
7) Quando sei connessi 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:
12) potresti essere accusato di cyberbullismo.
13) Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE.
14) 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.
15) Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori.
16) Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.
17) Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa.
18) Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori.
19) Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

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 policy e-safety 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 informateli 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 su Internet del laboratorio (qualora sia stata attivata).
6) Ricordate agli alunni che la violazione consapevole della policy e-safety della scuola, di utilizzo consentito della rete, 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 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.
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.
10) Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo 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

1) 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 "parentalcontroll" attraverso la sezione sicurezza in internet dal pannello di controllo.
6) Attivate il firewall (protezione contro malware) 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) Partecipate alle esperienze on line: navigate insieme a vostro figlio, incontrate amici on line, discutete 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.

2) Consigli in base all'età

Se tuo figlio/a ha meno di 8 anni:
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;
Comunica a tuo 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: insegna a tuo 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. Insegna a tuo figlio come registrarsi senza rivelare informazioni personali).

Se tuo figlio/a ha tra gli 8 anni e i 10 anni:
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.
Verifica periodicamente i contenuti dei siti "sicuri".
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.
Supervisiona l'email di tuo figlio dopo averlo reso consapevole del fatto che hai pieno accesso alle sue comunicazioni.
Comunicagli che è assolutamente vietato cliccare su un link, contenuto in una E-mail, su un pop-up pubblicitario o su un banner (ricordati, infatti, che potrebbero presentarsi immagini pornografiche o che potrebbe avviarsi il download di "malware").
Incoraggia l'uso di internet per svolgere ricerche scolastiche. 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? 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.
Aiuta tuo figlio a creare una rete on line sicura: siti controllati ed amici conosciuti

Se tuo figlio ha oltre 13 anni:
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.
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.
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.
Il computer deve rimanere in una stanza accessibile a tutta la famiglia e non nella camera di tuo figlio ALMENO fino ai 16 anni.

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

Non vi sono protocolli siglati ma ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullimo con l'Amministrazione Comunale, Comando dei Carabinieri e le Forze di Polizia, il Telefono Azzurro.